2002 Human-Technology Integration Colloquium Series
Air Force Research Laboratory
Human Effectiveness Directorate

Barrier Analysis and Accident Prevention

Erik Hollnagel, PhD
University of Linköping

16 May 2002 2:00 PM

Understanding and predicting accidents

'My dear friend Copperfield,' said Mr. Micawber,
...
'Accidents will occur in the best-regulated families;
...
they may be expected with confidence, and must be borne with philosophy.'

Systems; organisations

The probability that a specified event will occur.

The degree of certainty by which accidents can be expected.

The principles (models and theories) for describing and analysing accidents

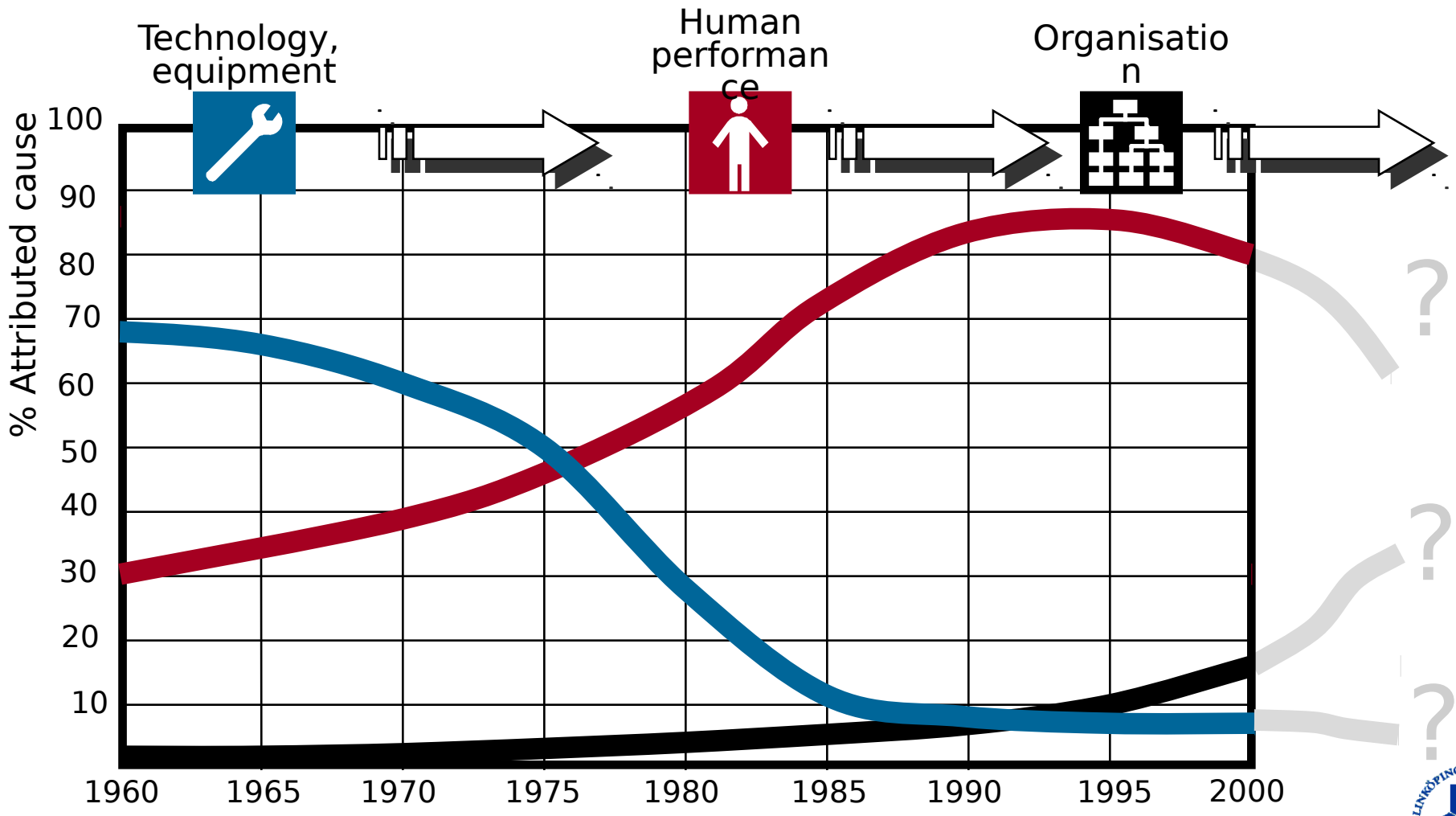
The lessons learned and the approaches to system design (prevention, protection).

Charles Dickens
David Copperfield
(1850) Chapter 28

Erik Hollnagel, 2002

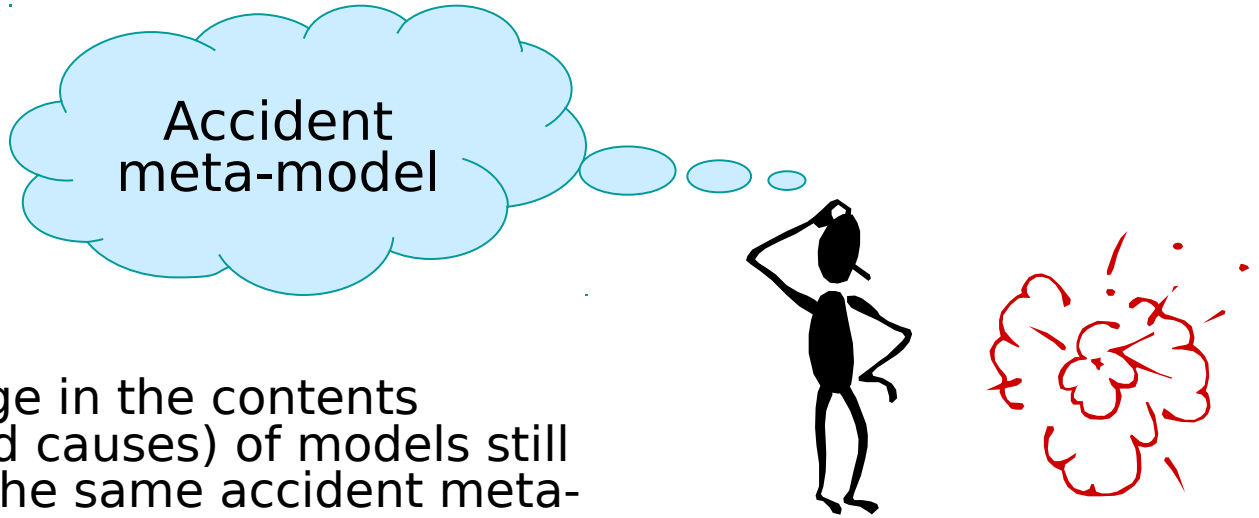
LINKÖPINGS UNIVERSITET

Changes in attributed cause types

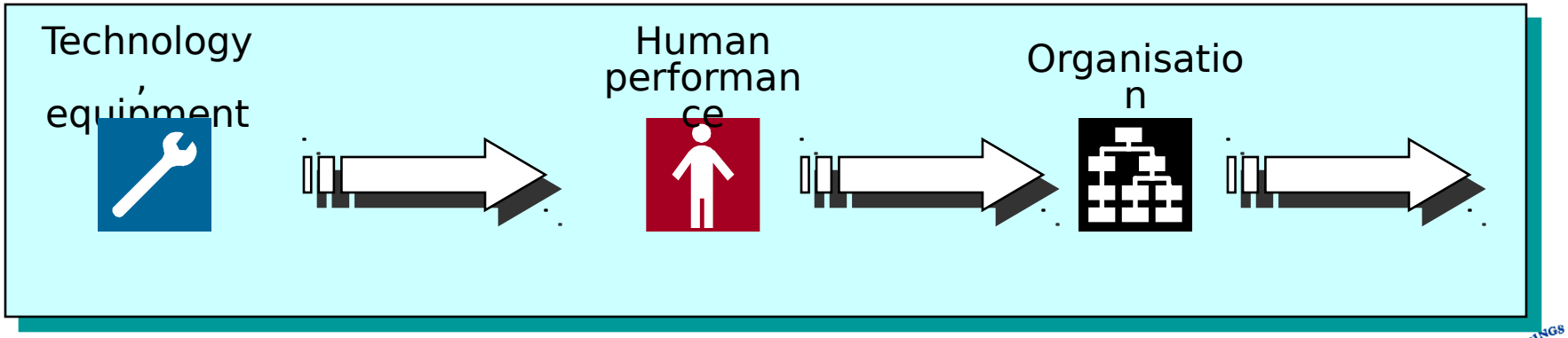


Erik Hollnagel, 2002

Model contents and model form

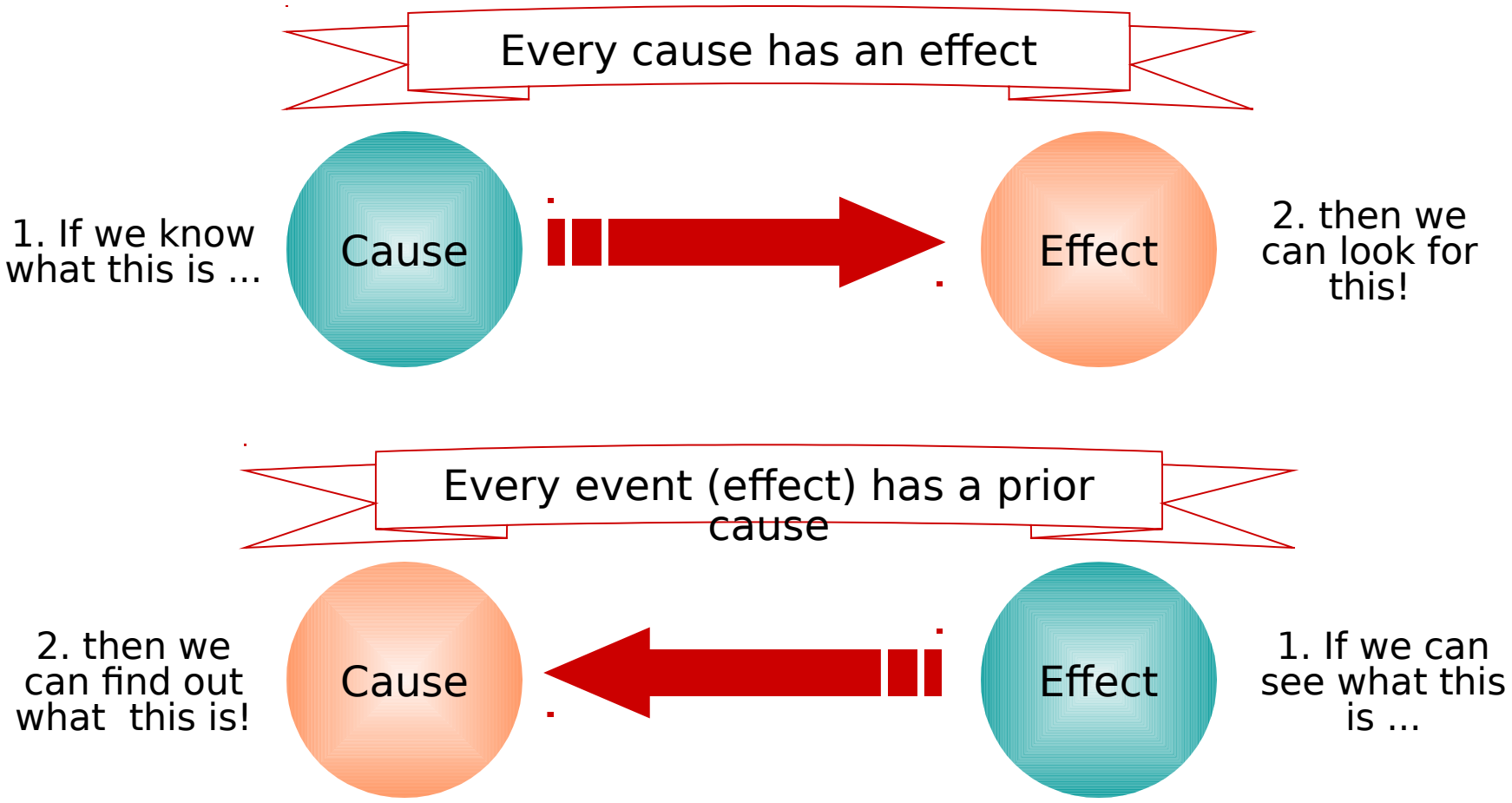


The change in the contents (attributed causes) of models still refers to the same accident meta-model.



Erik Hollnagel, 2002

Causality assumption

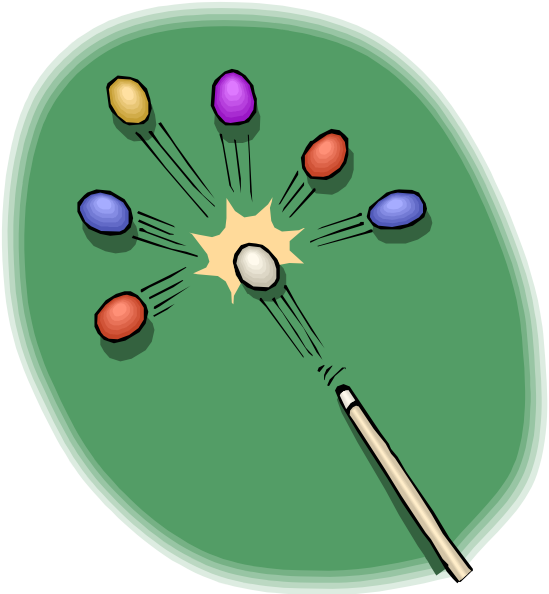

Every cause has an effect
1. If we know what this is ...
Cause
Effect
2. then we can look for this!
Every event (effect) has a prior cause
2. then we can find out what this is!
Cause
Effect
1. If we can see what this is ...

Erik Hollnagel, 2002

Cause and effect

Isaac Newton: Classical mechanics, clear relations between cause and effect (1st, 2nd, 3rd Law)

David Hume: Causality = priority in time of cause to effect, contiguity in space and time, necessary connection

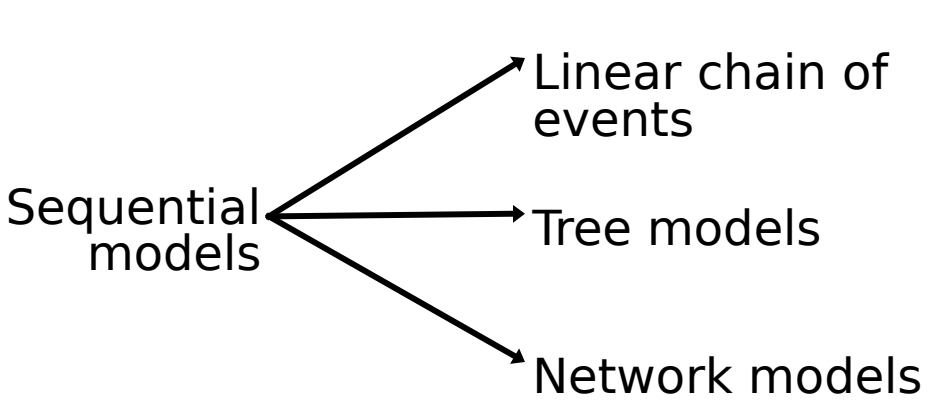


Willard Gibbs: Statistical mechanics, probabilistic relations between cause and effect

Non-linear dynamics (chaos theory): Confluence, coincidence

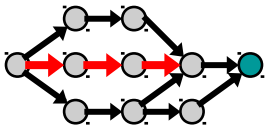
Erik Hollnagel, 2002

Sequential accident models



Domino model

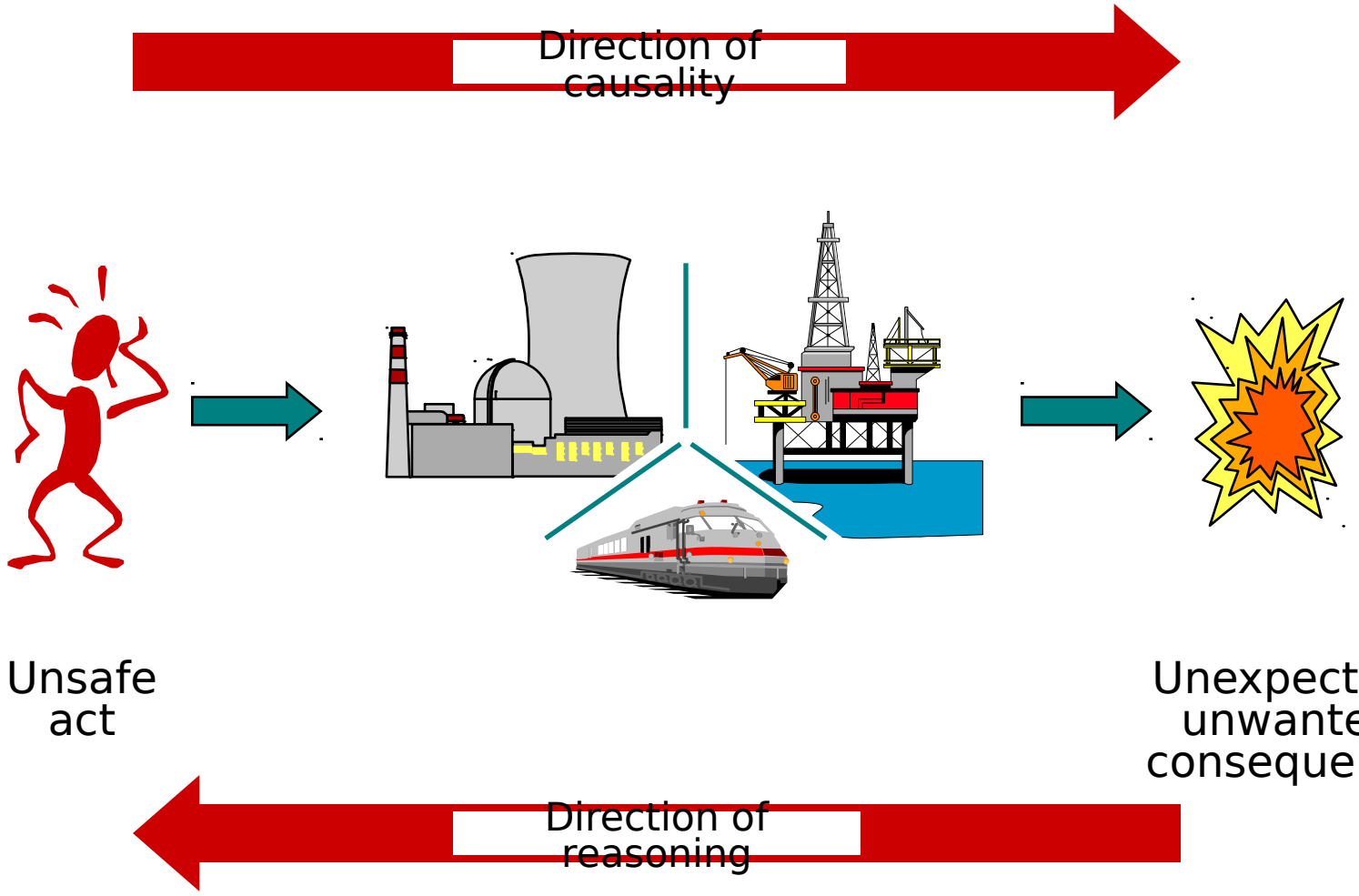
Event tree


Critical path

Principle of accident analysis	Goal of accident analysis
Search for recognisable, specific causes and well-defined cause effect links.	Causes - when found - can be eliminated or contained.

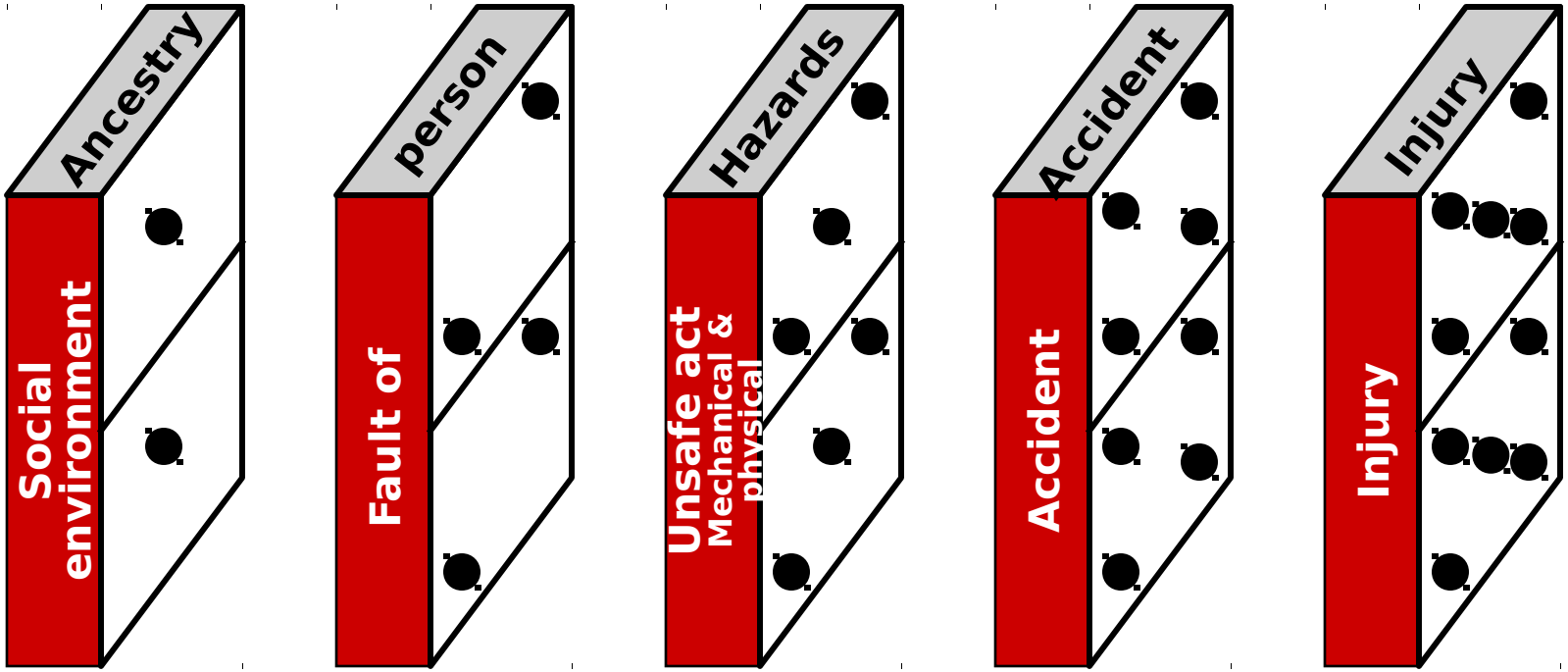
Erik Hollnagel, 2002

Sequential accident model



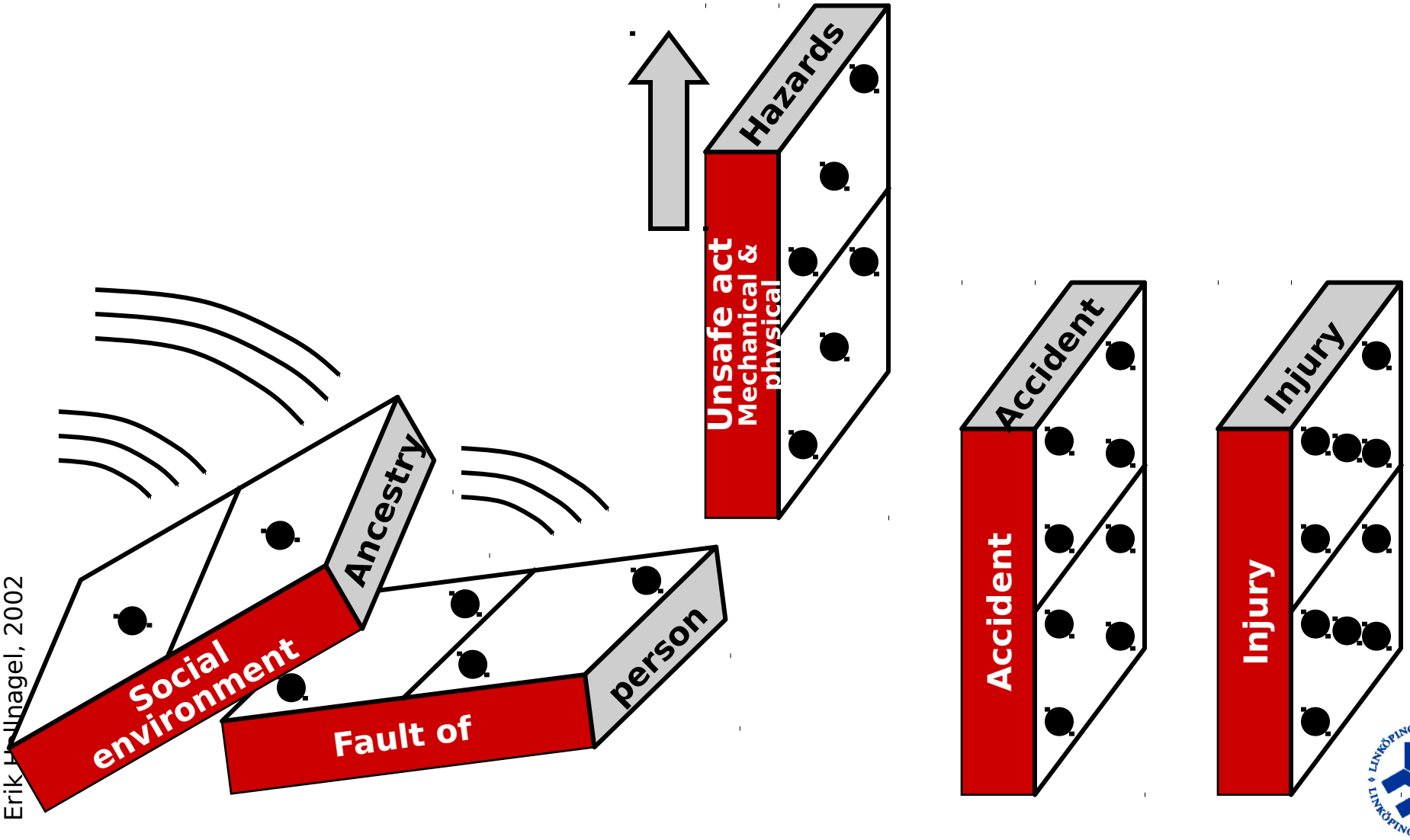
Erik Hollnagel, 2002

Domino model (Heinrich, 1930)



Erik Hollnagel, 2002

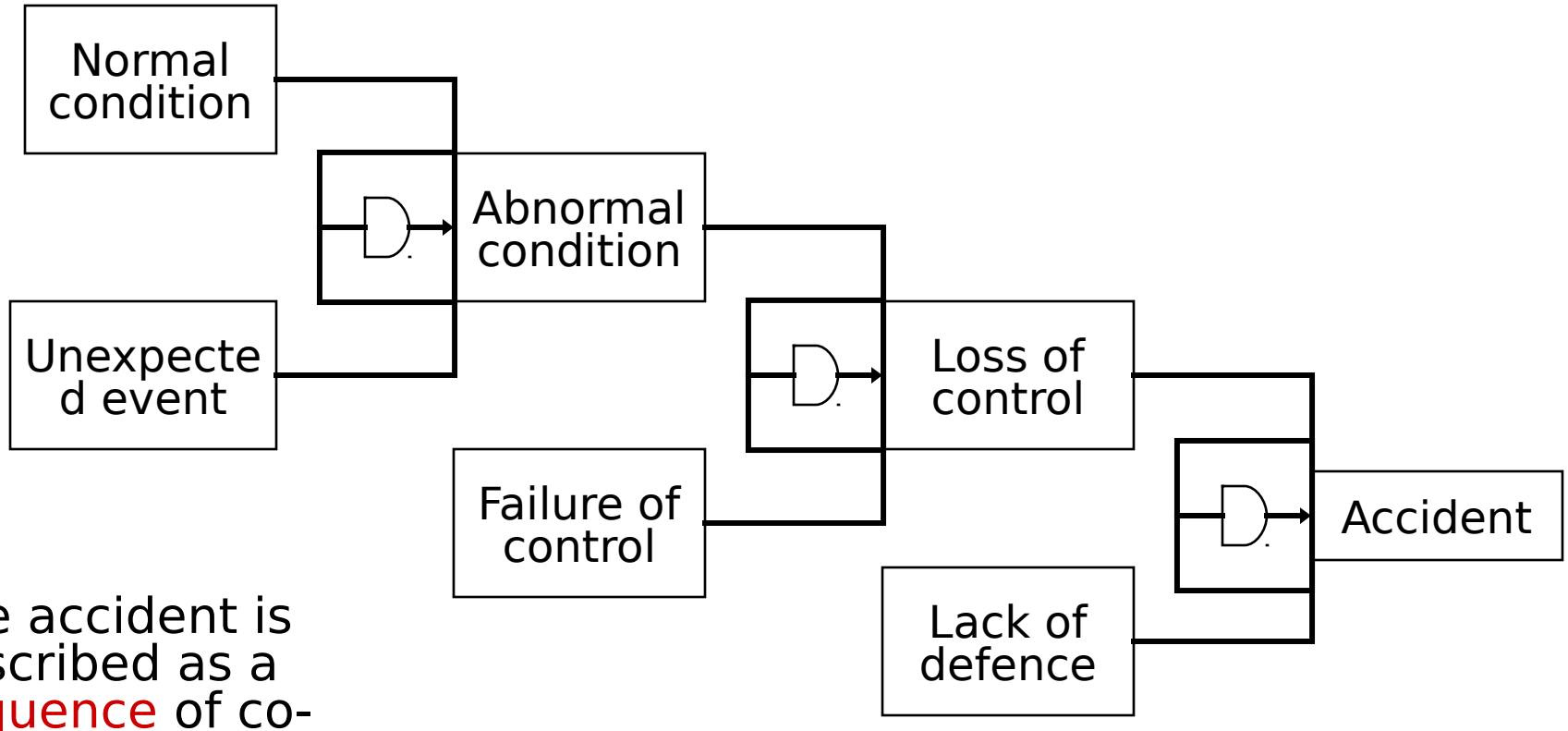
Domino model - cause elimination



Erik Hollnagel, 2002

Anatomy of an accident

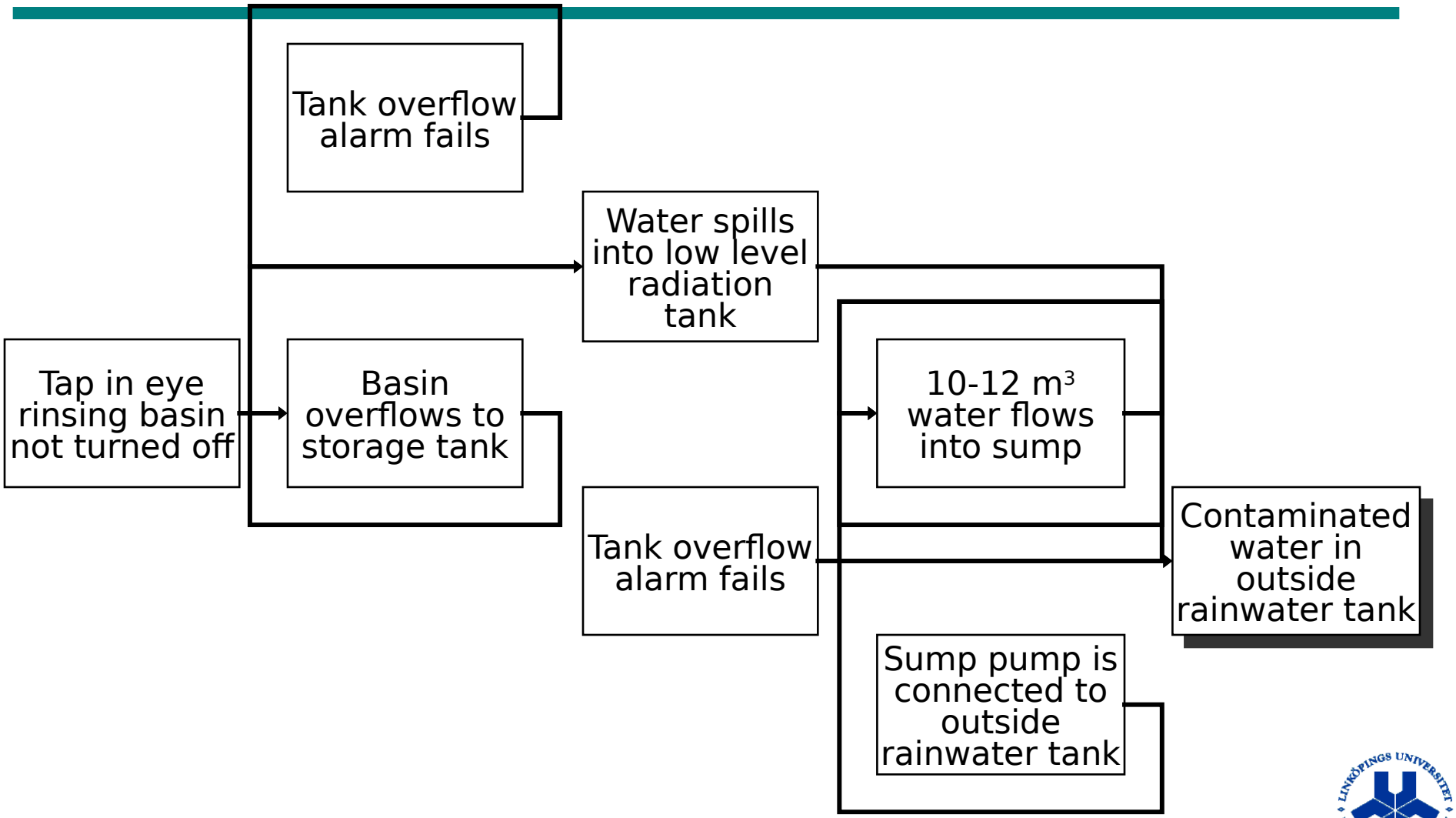
Green, 1988



The accident is described as a sequence of co-occurring events / conditions

Erik Hollnagel, 2002

Spill at Cadarache (F)

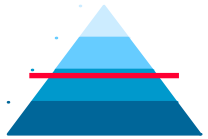

Tank overflow alarm fails
Water spills into low level radiation tank
Tap in eye rinsing basin not turned off
Basin overflows to storage tank
10-12 m3 water flows into sump
Tank overflow alarm fails
Contaminated water in outside rainwater tank
Sump pump is connected to outside rainwater tank

Erik Hollnagel, 2002

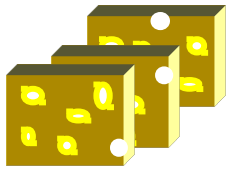
Epidemiological accident models

Epidemiological models

- Latent conditions
- Carriers-barriers
- Pathological systems



Iceberg model



Swiss cheese model

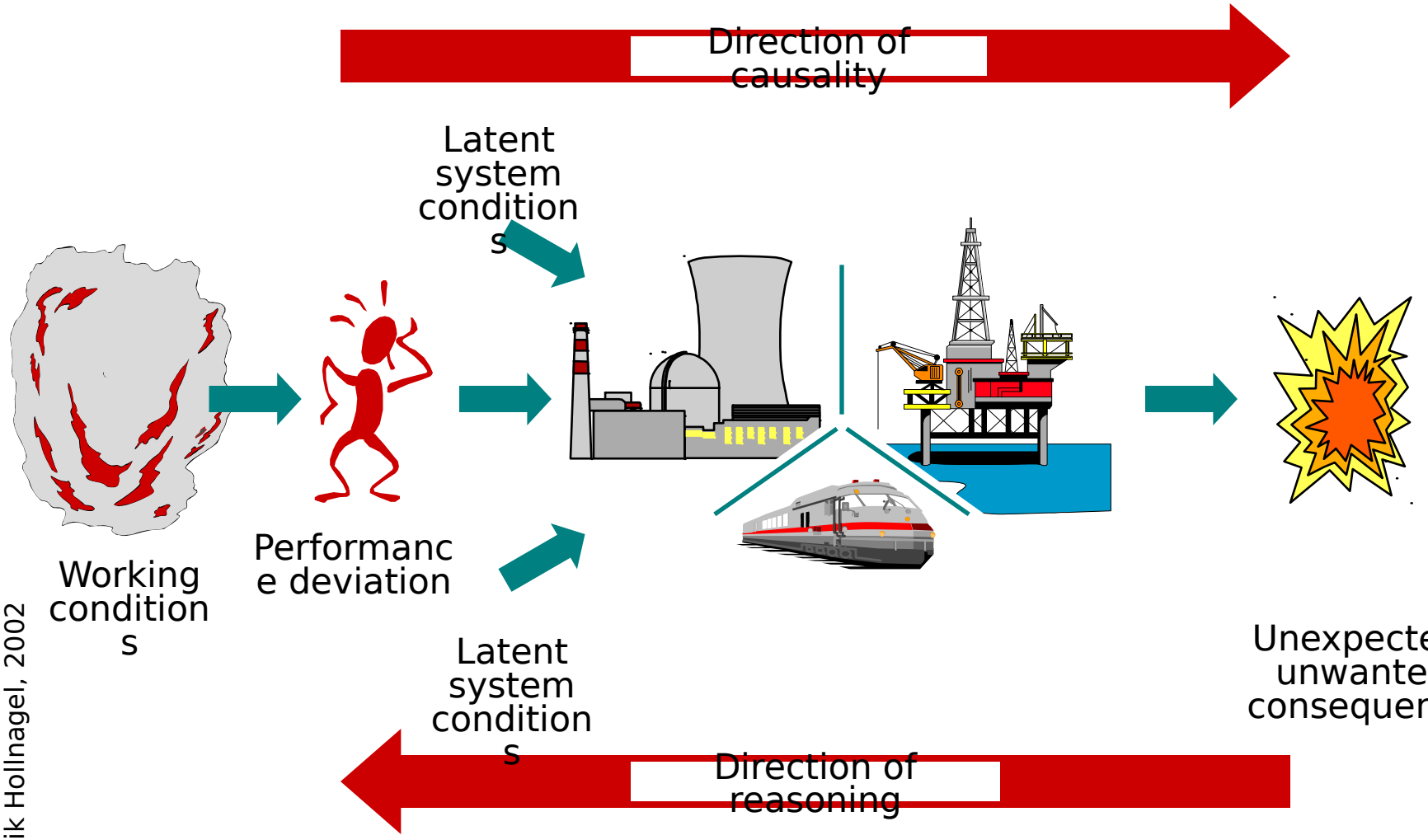
Principle of accident analysis	Goal of accident analysis
Search for “carriers” and latent conditions; define indications of general system “health”.	Make defences and barriers stronger.

… but … causality cannot be attributed solely on the basis of a temporal relation (A prior to B)

Erik Hollnagel, 2002

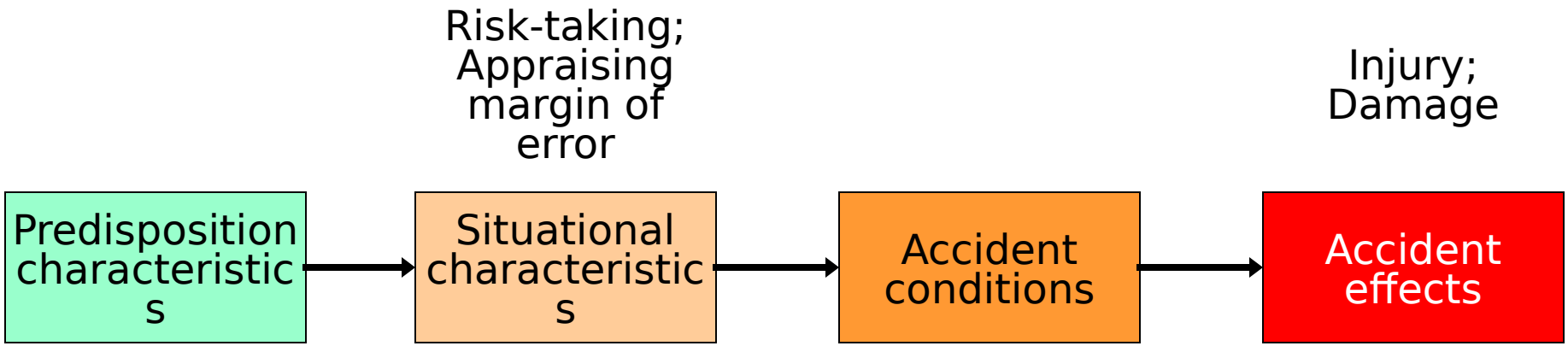
LINKÖPINGS UNIVERSITET

Epidemiological accident model



Erik Hollnagel, 2002

Epidemiological model (Suchman, 1960)



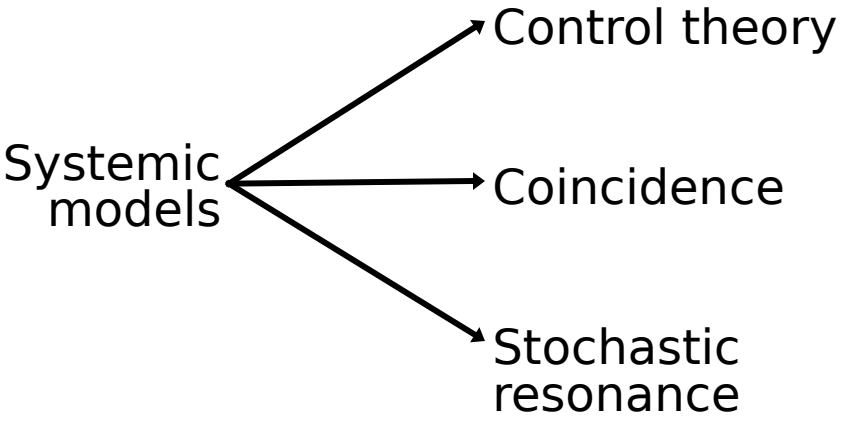
Erik Hollnagel, 2002

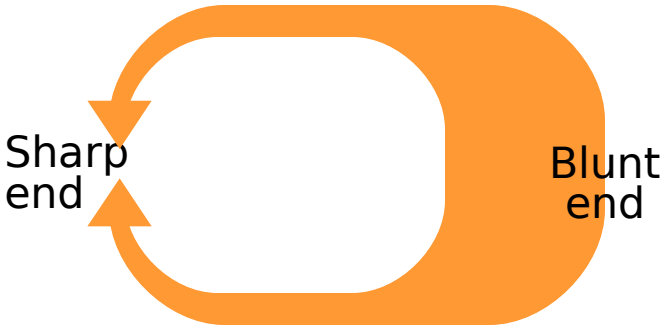
NY Subway Crash

- A NYC subway train on the Williamsburg Bridge crashed into the rear end of another train on 5 June 1995.
  - Motorman apparently ran through a red light, was still applying power at time of crash. Motorman was killed, 54 were injured.
- ATC is supposed to apply emergency brakes whenever a train runs a red light. The brakes did work, but:
  - Distance to train ahead was 288 ft
  - Breaking distance at 32 mph is 360 ft
  - Collision speed was about 14-18 mph
- Signal spacing was defined in 1918 (sic).
  - At that time trains were shorter, lighter, and slower than modern trains.
- Trains had been upgraded, but control systems had not.

LINKÖPINGS UNIVERSITET

Systemic accident models

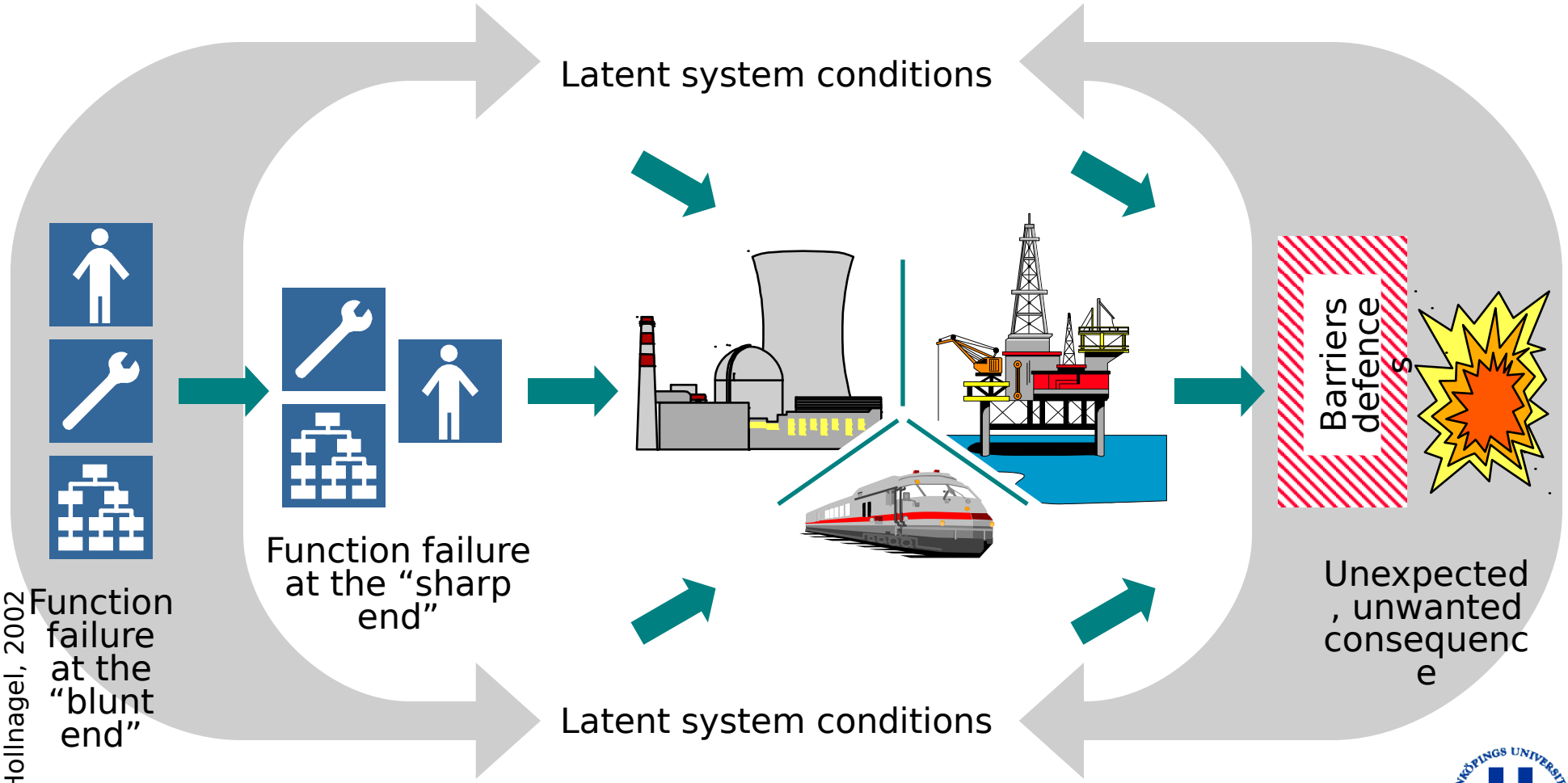




Principle of accident analysis	Goal of accident analysis
Search for unusual dependencies and "common conditions"	Performance variability can be detected and controlled

Erik Hollnagel, 2002

Systemic accident model


Latent system conditions
Function failure at the "blunt end"
Function failure at the "sharp end"
Barriers defence s
Unexpected , unwanted consequenc e
Latent system conditions

Erik Hollnagel, 2002

M/S Stockholm – July 20, 2000

Captain + first officer on bridge

Two crewmembers (AB) in engine room

One AB accidentally shuts off fuel to main generator

Complete loss of electrical power

Captain connects shaft generator

Captain sets pitch control = 0; rudder to port to avoid rock face

Captain tries to reconnect SG

First officer turns off unnecessary electrical equipment (galley, etc.)

Captain stops engines; emergency clutch out

Emergency generator started

SG overload trip after 10 seconds

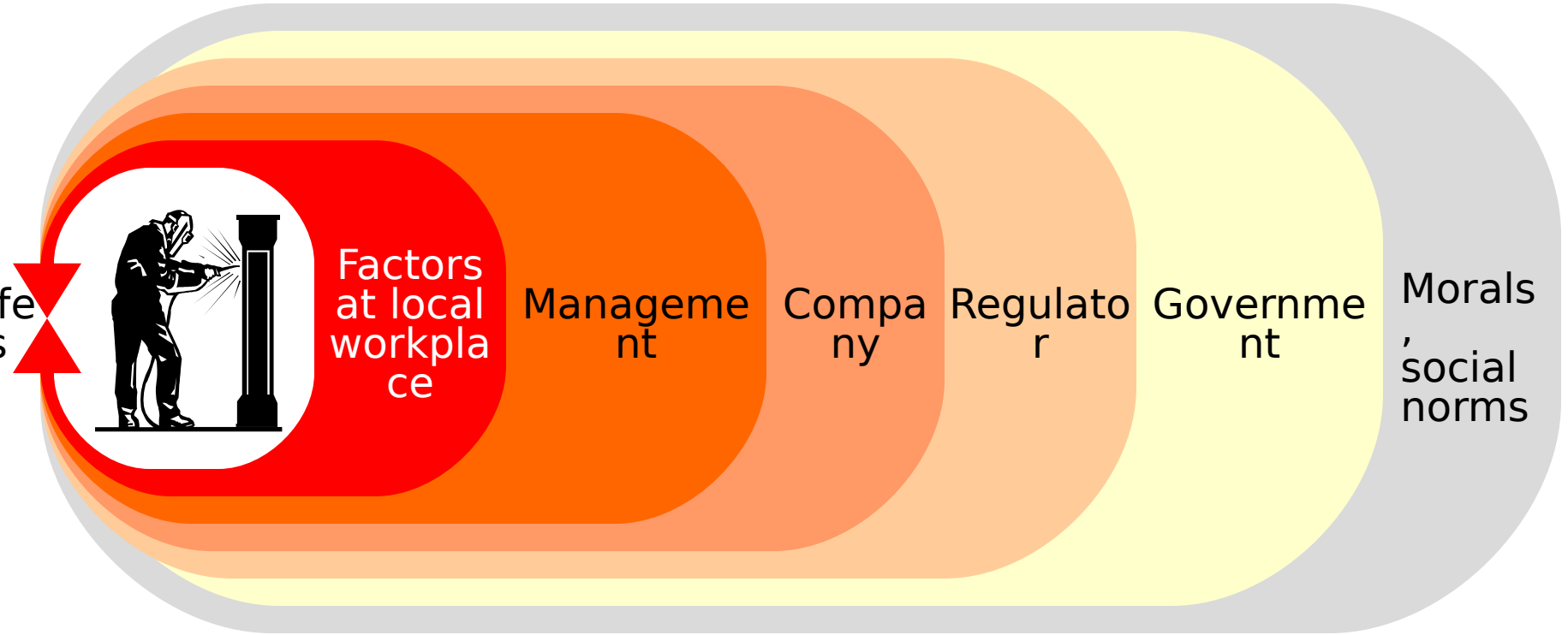
Emergency generator does not start

Grounding of M/S Stockholm

Erik Hollnagel, 2002

LINKÖPINGS UNIVERSITET

Sharp end - blunt end



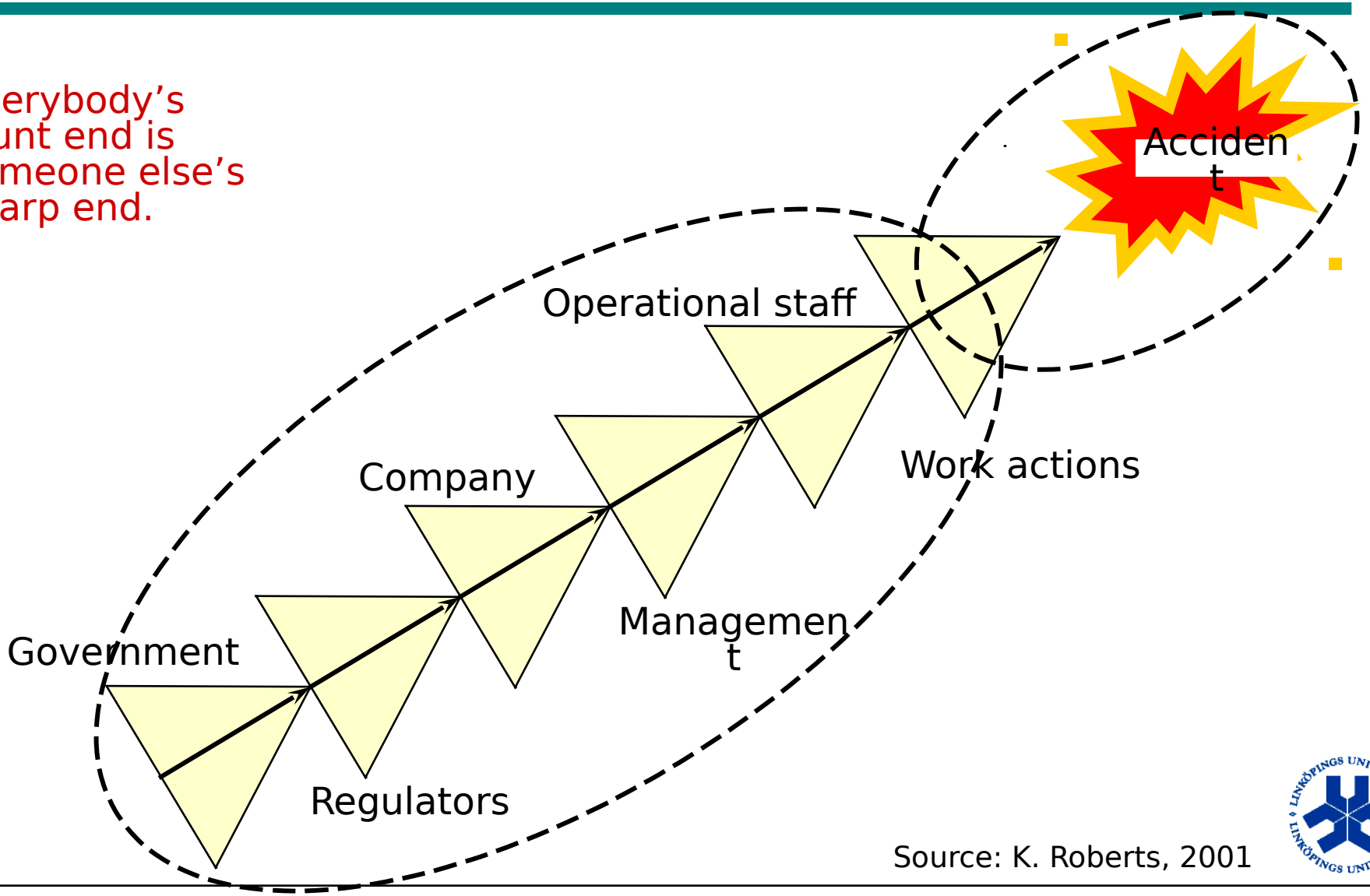
"Sharp end" factors work here and now

"Blunt end" factors are removed in space and time

Erik Hollnagel, 2002

Sharp-end - blunt-end

Everybody's blunt end is someone else's sharp end.



Source: K. Roberts, 2001

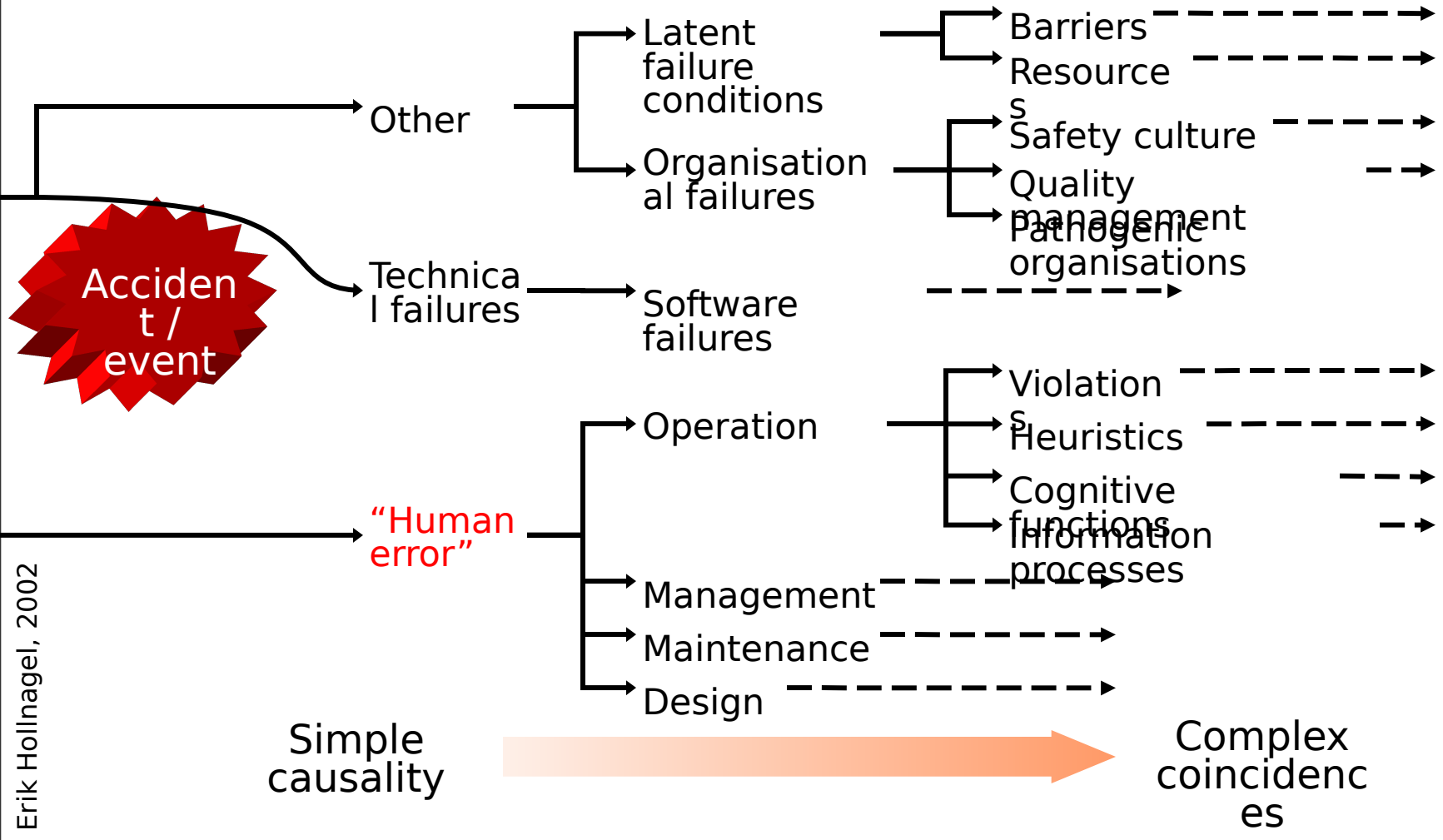
Erik Hollnagel, 2002

Accident meta-models

	Sequential accident model	Epidemiological accident model	Systemic accident model
Search principle of accident analysis	Specific causes and well-defined links.	Carriers, barriers, and latent conditions.	Functional dependencies and common conditions
Goal of accident analysis	Eliminate or contain causes.	Strengthen defences and barriers .	Monitor & control performance variability

Erik Hollnagel, 2002

Evolving concept of causes



Erik Hollnagel, 2002

Axioms of industrial safety (1-5)

1. The occurrence of an injury invariably results from a completed sequence of factors - the last one of these being the accident itself. The accident in turn is invariably caused or permitted directly by the unsafe act of a person and/or a mechanical or physical hazard.

2. The unsafe acts of persons are responsible for a majority of accidents.

3. The person who suffers a disabling injury caused by an unsafe act, in the average case has had over 300 narrow escapes from serious injury as a result of committing the very same unsafe act. Likewise, persons are exposed to mechanical hazards hundreds of times before they suffer injury.

4. The severity of an injury is largely fortuitous - the occurrence of the accident that results in injury is largely preventable.

5. The four basic motives or reasons for the occurrence of unsafe acts provide a guide to the selection of appropriate corrective measures.

Erik Hollnagel, 2002

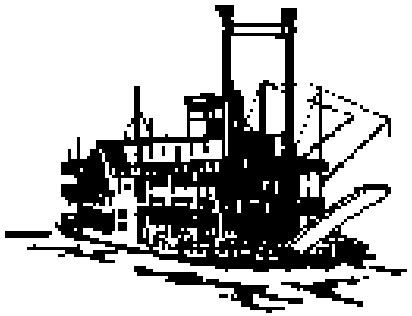
LINKÖPINGS UNIVERSITET

Axioms of industrial safety (6-10)

6	Four basic methods … for preventing accidents - engineering revision, persuasion and appeal, personnel adjustment, and discipline.
7	Methods of most value in accident prevention are analogous with the methods required for the control of the quality, cost, and quantity of production.
8	Management has the best opportunity and ability to initiate the work of prevention; therefore it should assume the responsibility.
9	The supervisor or foreman is the key man in industrial accident prevention. His … … supervision to the control of worker performance is the factor of greatest influence in successful accident prevention. …
10	The humanitarian incentive for preventing accidental injury is supplemented by two powerful economic factors: (1) the safe establishment is efficient productively and the unsafe establishment is inefficient; (2) the direct employer cost of industrial injuries for compensation claims and for medical treatment is but one-fifth of the total cost which the employer must pay.

LINKÖPINGS UNIVERSITET

Exploding steam engines



US 1816-1848

233 steamboat explosions
2.562 persons killed; 2.097 injured
Property loss in excess of 3.000.000 $

Most accidents were blamed on owners and operators.

BUT

Boiler technology lagged behind improvements in steam engines.

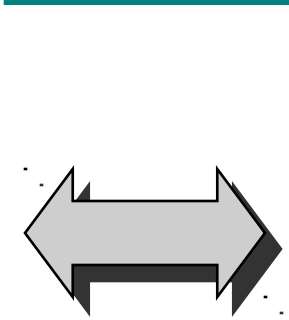
Little understanding of build-up of steam pressure, effects of corrosion, causes of boiler explosions.

Engineers lacked proper training and skills.

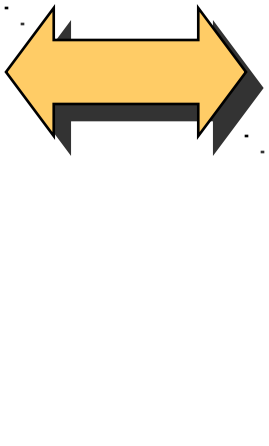
Erik Hollnagel, 2002

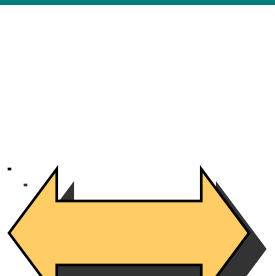
LINKÖPINGS UNIVERSITET

Counterfactual reasoning

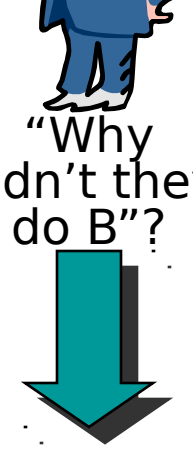


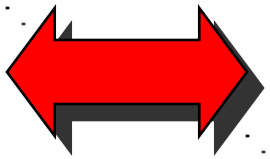
"Why didn't they do A"?





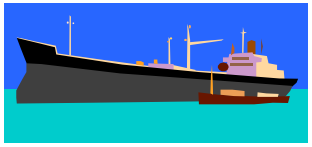
"Why didn't they do B"?

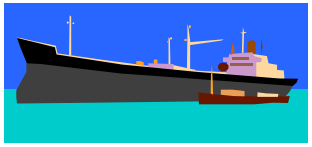




Actual outcome

Possible outcome 1





Possible outcome 2

Going back through a sequence, investigators often wonder why opportunities to avoid the bad outcome were missed. This, however, does not explain the failure

Erik Hollnagel, 2002

LINKÖPINGS UNIVERSITET

Performance deviations

"Knowledge and error flow from the same mental sources, only success can tell one from the other."
(Mach, 1905)

Human performance is inherently variable!

Work conditions are inherently variable!

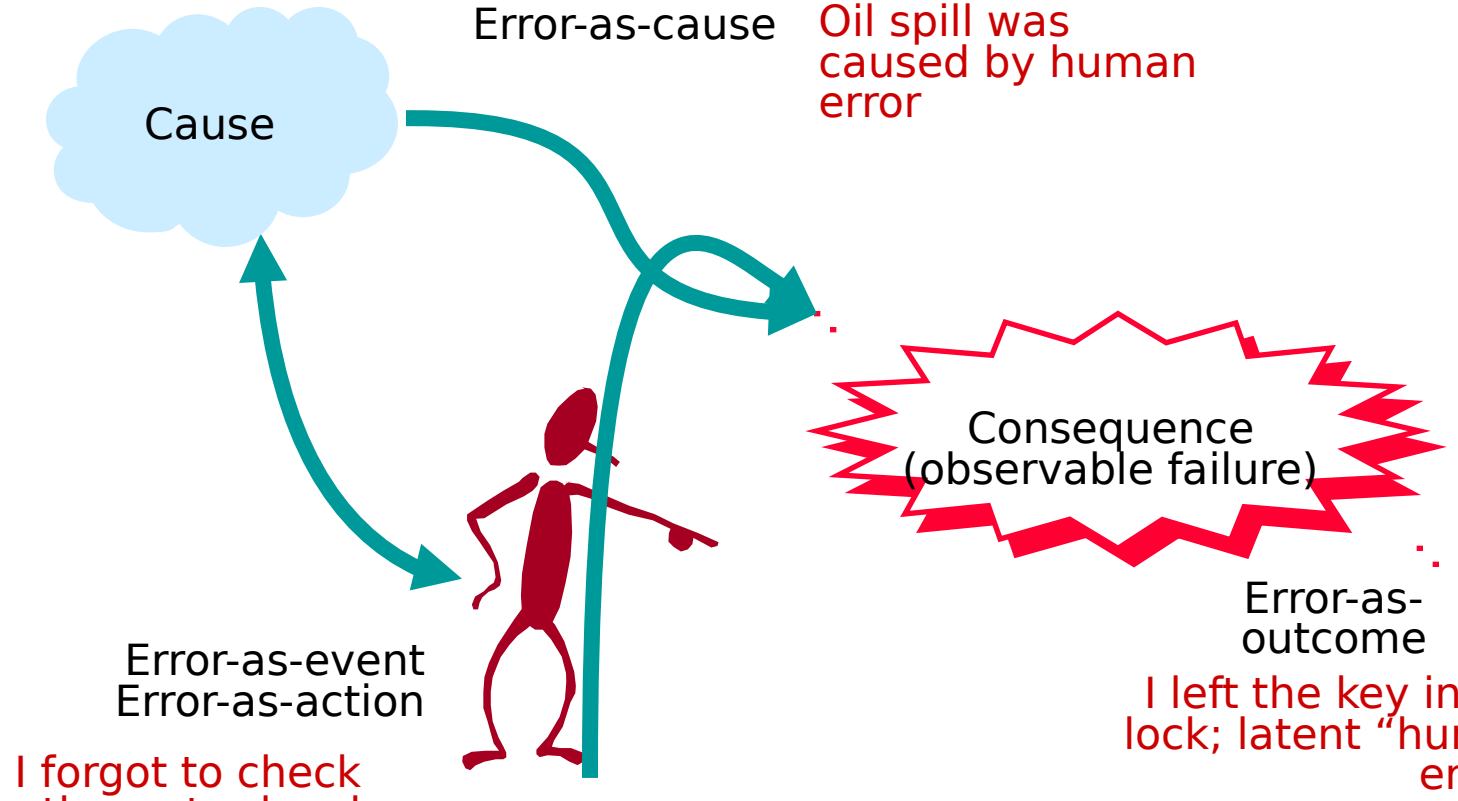
Actions with a negative outcome.
HUMAN ERROR!

Actions with a beneficial outcome.
CREATIVITY, LEARNING

Both types are performance deviations, and may have the same "causes"

Erik Hollnagel, 2002

Multiple meanings of “error”



Erik Hollnagel, 2002

What is an “error”?

Correctly performed actions

Actual outcomes = intended outcomes

Failure detected and recovered

Failure detected but tolerated

Failure detected but not recovered

Failure not detected

Actual outcomes ≠ intended outcomes

Immediate effects

Latent effects

Erik Hollnagel, 2002

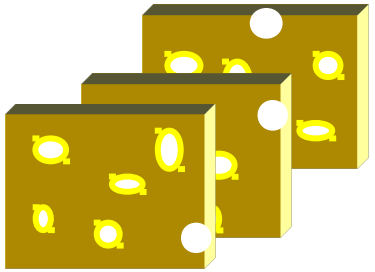
A cynical definition of causes

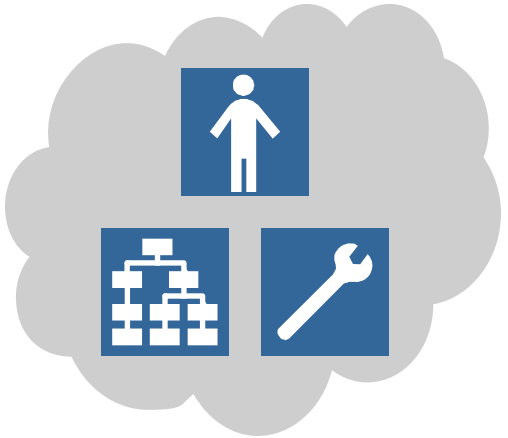
- A “cause” is the identification, after the fact, of a limited set of aspects of the situation that are seen as the necessary and sufficient conditions for the effect(s) to have occurred.
- A “cause” has the following characteristics:
  - It can unequivocally be associated with a system structure or function (people, components, procedures, etc.)
  - It is possible to do something to reduce or eliminate the cause within accepted limits of cost and time.
  - It conforms to the current “norms” for explanations.
- The determination of the “cause” is a relative (pragmatic) rather than absolute (scientific) process.

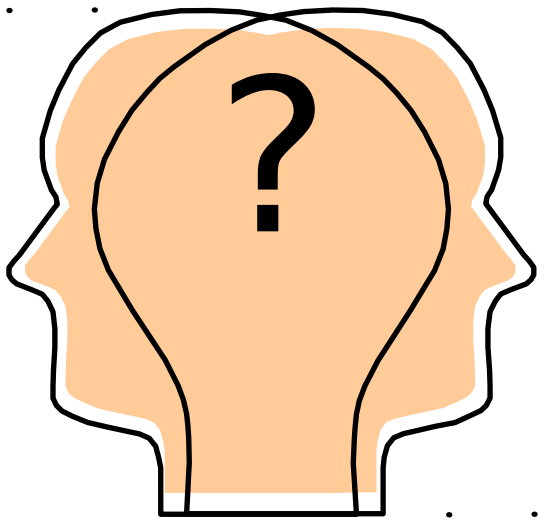
Erik Hollnagel, 2002

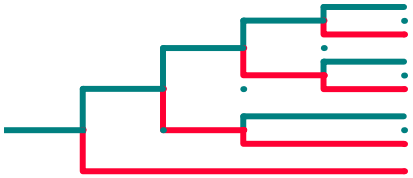
LINKÖPINGS UNIVERSITET

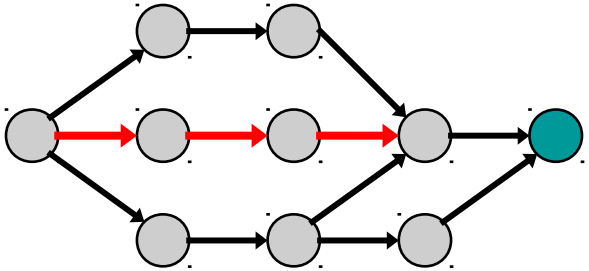
Analysis-prediction dilemma











Looking back, we acknowledge that accidents reflect complex coincidences

Looking ahead, accident “models” are still mostly linear or sequential.

Erik Hollnagel, 2002

Accident prevention

To prevent accidents, we must know:

What	Which types of accidents are possible in a system?
Where	Where in the system can accidents occur?
How	What are the “mechanisms” of an accident?
When	Under which conditions are accidents likely?

Are there any known or valid indicators for accident build-up?

Are there effective means (barriers, defences) to guard against accidents?

Erik Hollnagel, 2002

LINKÖPINGS UNIVERSITET

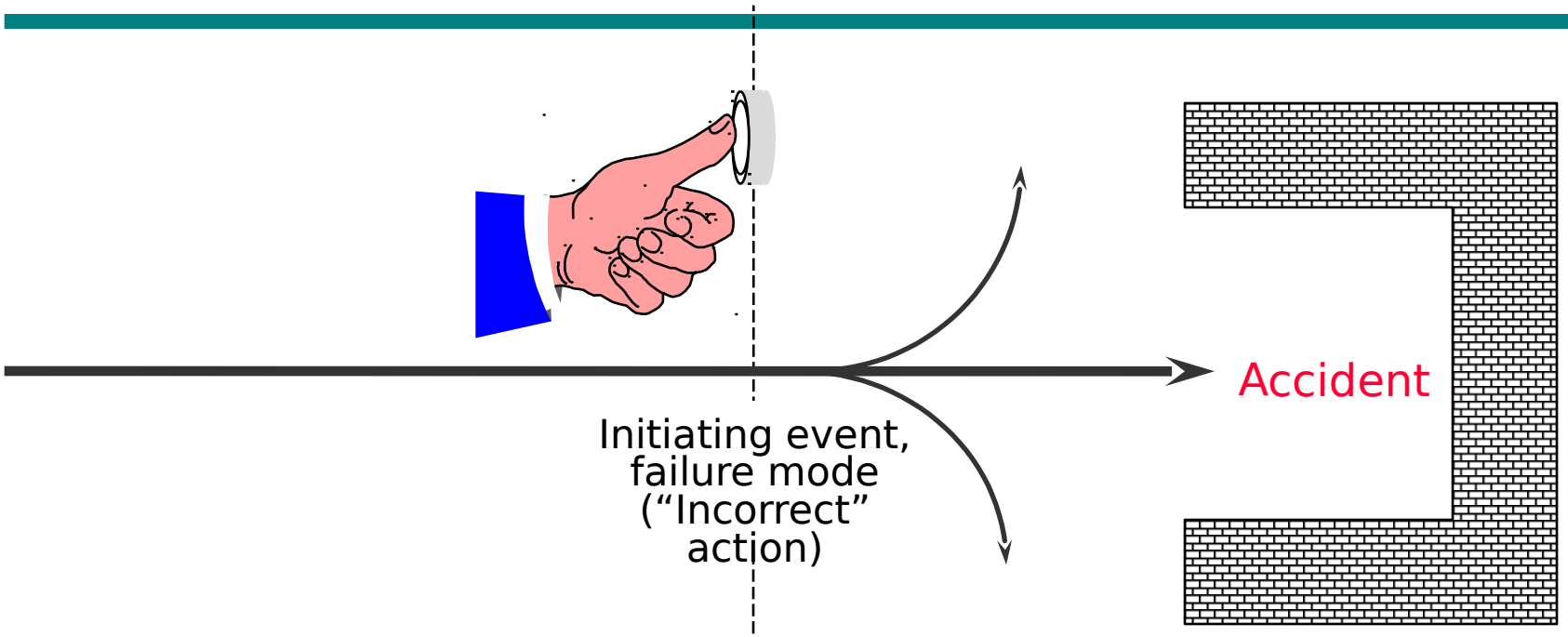
Barriers and safety

- Barrier purposes (WHY)
  - a barrier is an obstacle, obstruction or hindrance that may:
  - prevent an action or event from taking place
  - protect against or diminish the negative consequences of an action or event that has taken place.
- Barrier function (WHAT)
  - The specific manner by which the barrier achieves its purpose
- Barrier system (HOW)
  - The foundation or basis for the barrier function, the required organisational and/or physical structure
  - Barriers can be single or combined (defence-in-depth)
- Barriers are effective even if the cause is unknown or uncertain.

Erik Hollnagel, 2002

LINKÖPINGS UNIVERSITET

Prevention and protection

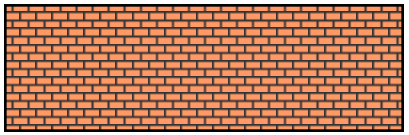


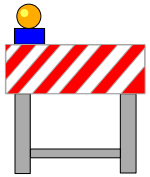
Prevention (control barriers):	Protection (safety barriers):	Protection (boundaries):
Active or passive barrier functions that prevent the initiating event from occurring.	Active barrier functions that deflect consequences	Passive barrier functions that minimise consequences

Erik Hollnagel, 2002

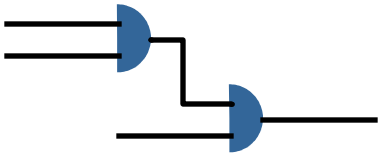
Barrier system types

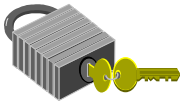
- Physical, material
  - Obstructions, hindrances, ...



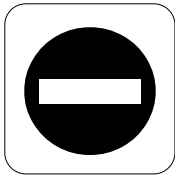


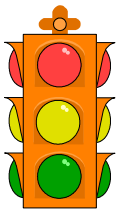
- Functional
  - Mechanical (interlocks)
  - Logical, spatial, temporal



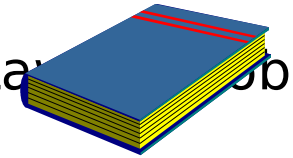


- Symbolic
  - Signs & signals
  - Procedures
  - Interface design





- Immaterial
  - Rules, laws, principles
  - Ten Commandments, La obotics



Erik Hollnagel, 2002

LINKÖPINGS UNIVERSITET

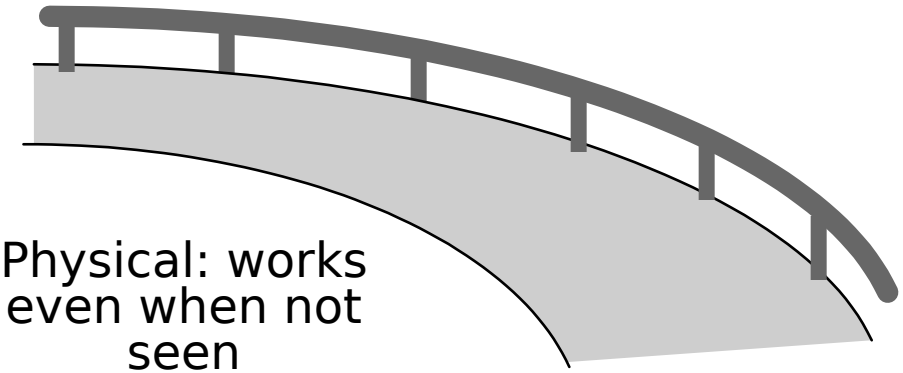
Types of barrier systems

- Material barriers
  - Physically prevents an action from being carried out, or prevents the consequences from spreading
- Functional (active or dynamic) barriers
  - Hinders the action via preconditions (logical, physical, temporal) and interlocks (passwords, synchronisation, locks)
- Symbolic barriers (perceptual, conceptual barriers)
  - Requires an act of interpretation to work, i.e. an intelligent and perceiving agent (signs, signals alarms, warnings)
- Immaterial barriers (non-material barriers)
  - Not physically present in the situation, rely on internalised knowledge (rules, restrictions, laws)

Erik Hollnagel, 2002

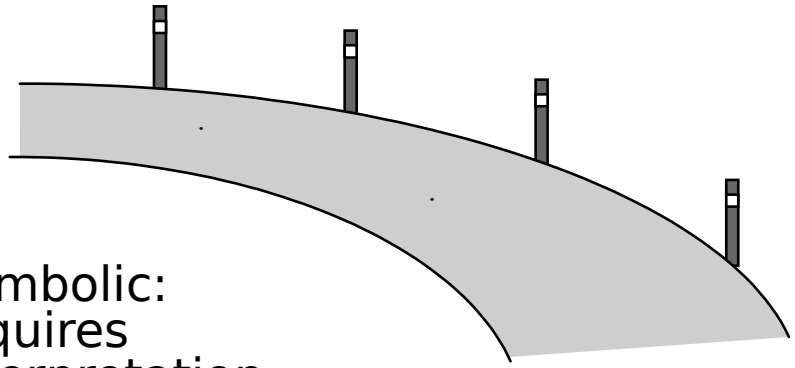
LINKÖPINGS UNIVERSITET

Barriers systems on the road

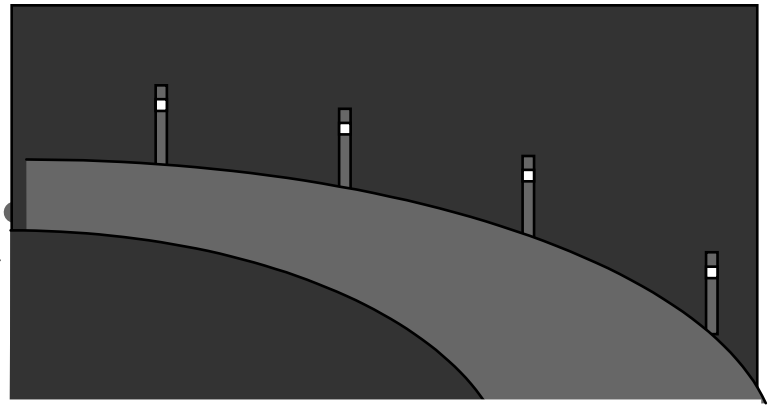


Physical: works even when not seen

Symbolic: requires interpretation



Symbolic: requires interpretation

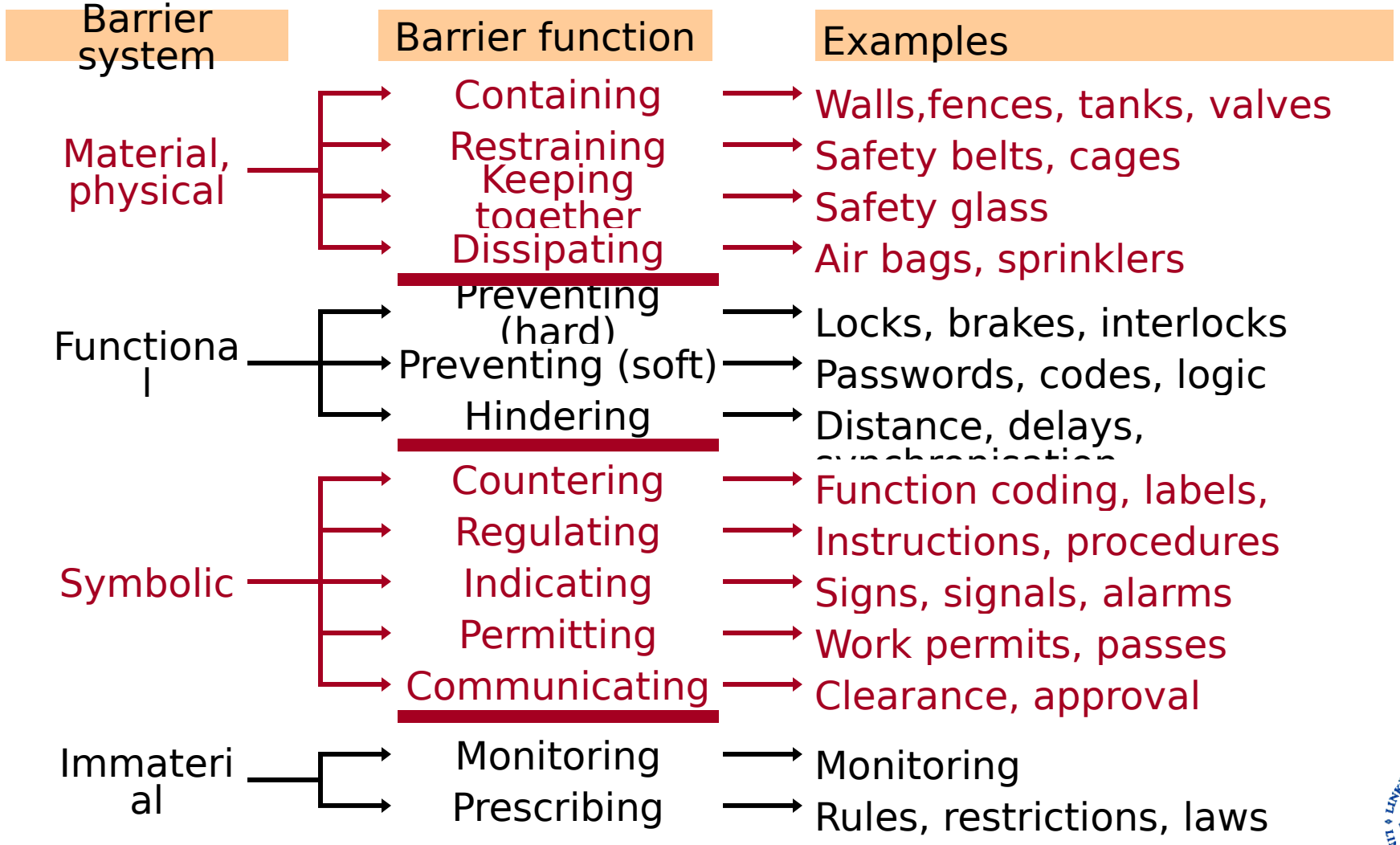


Symbolic: requires interpretation

Erik Hollnagel. 2002

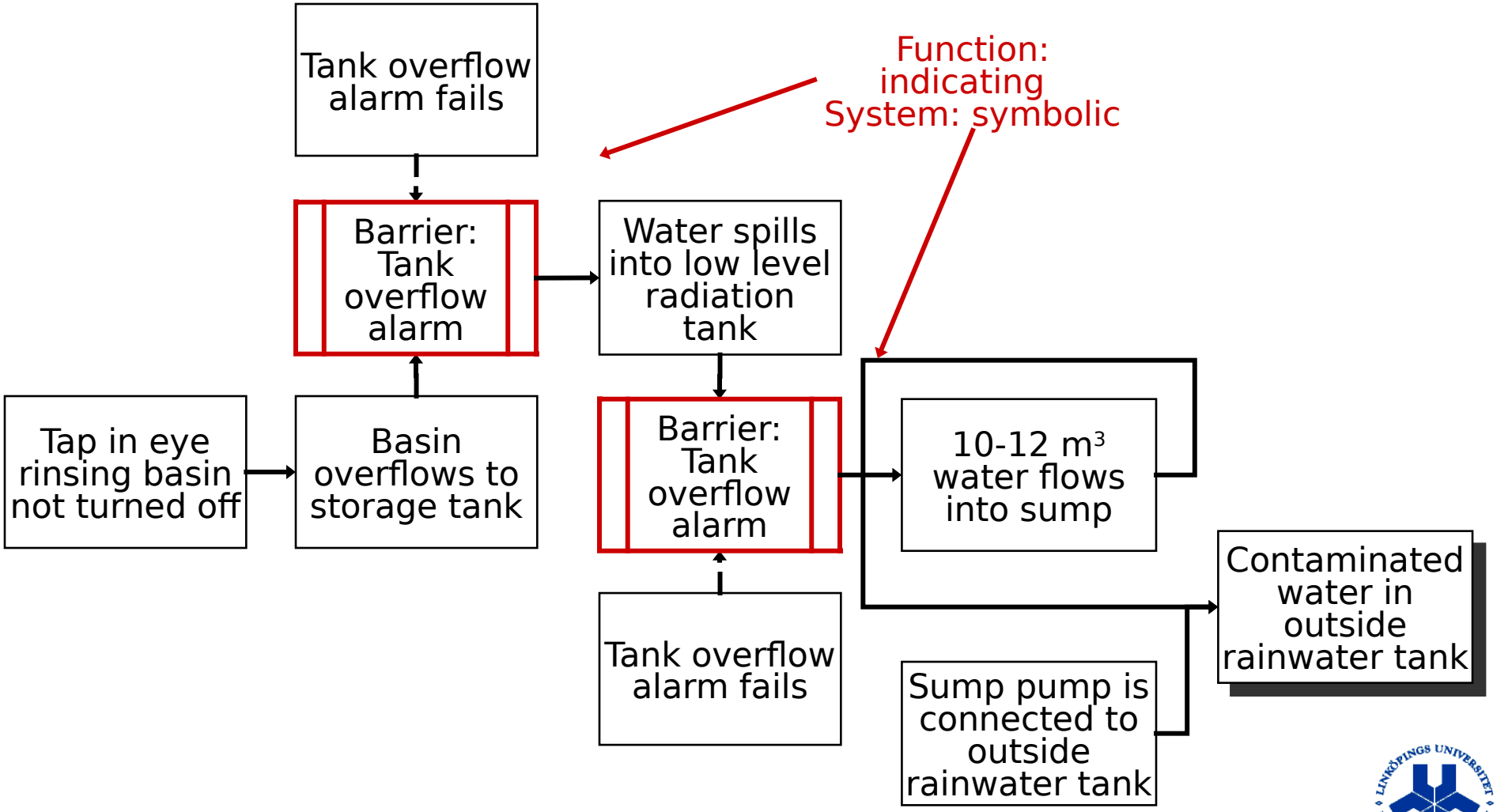
LINKÖPINGS UNIVERSITET

Barrier systems / barrier functions



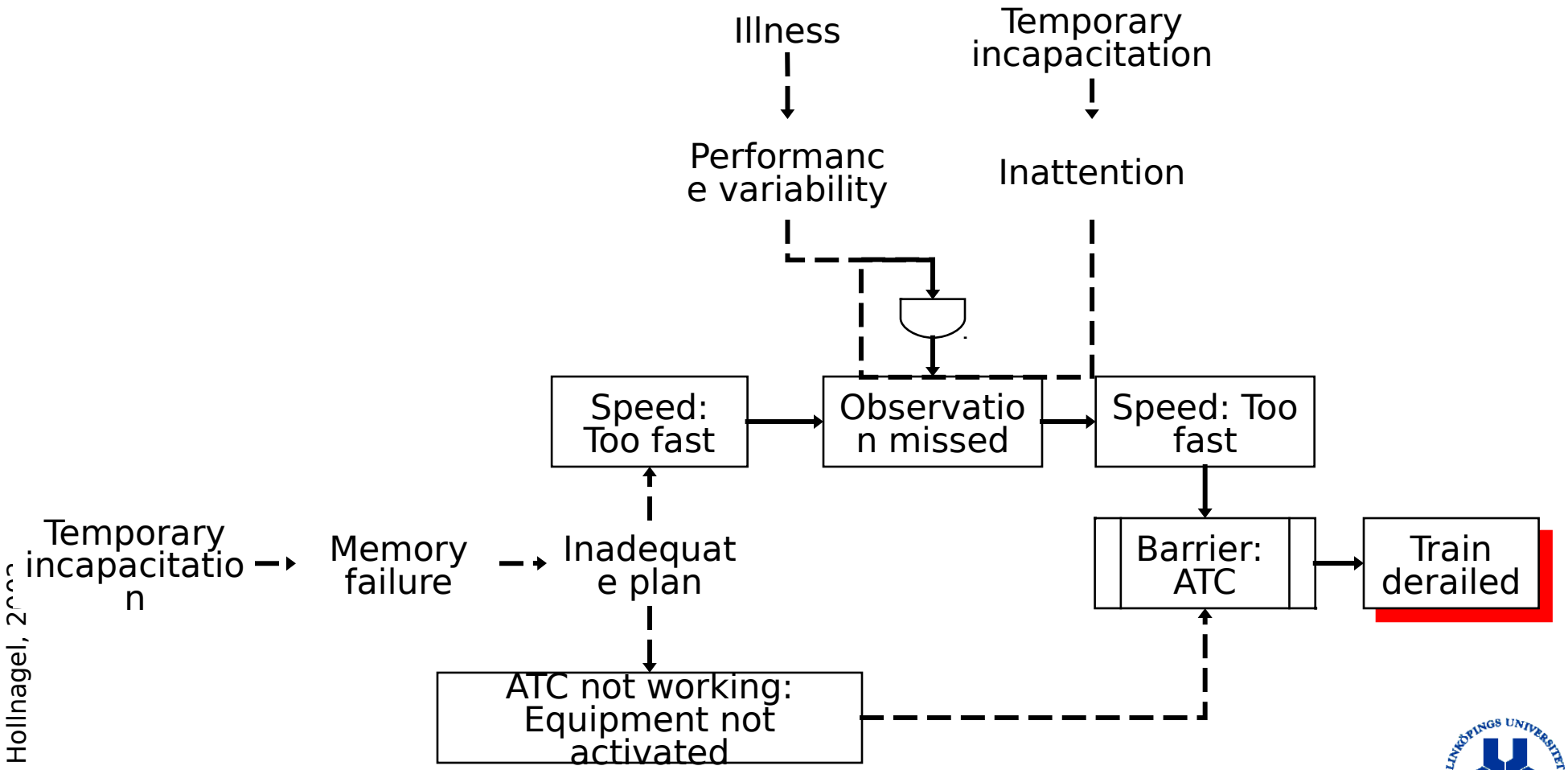
Erik Hollnagel, 2002

Spill at Cadarache (F)


Tank overflow alarm fails
Function: indicating System: symbolic
Barrier: Tank overflow alarm
Water spills into low level radiation tank
Tap in eye rinsing basin not turned off
Basin overflows to storage tank
Barrier: Tank overflow alarm
10-12 m3 water flows into sump
Contaminated water in outside rainwater tank
Tank overflow alarm fails
Sump pump is connected to outside rainwater tank

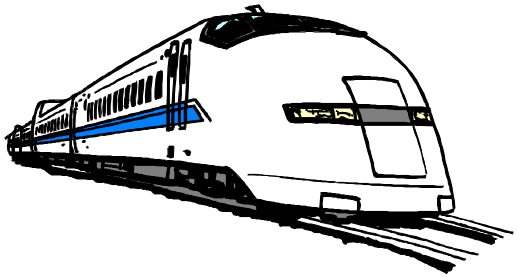
Erik Hollnagel, 2002

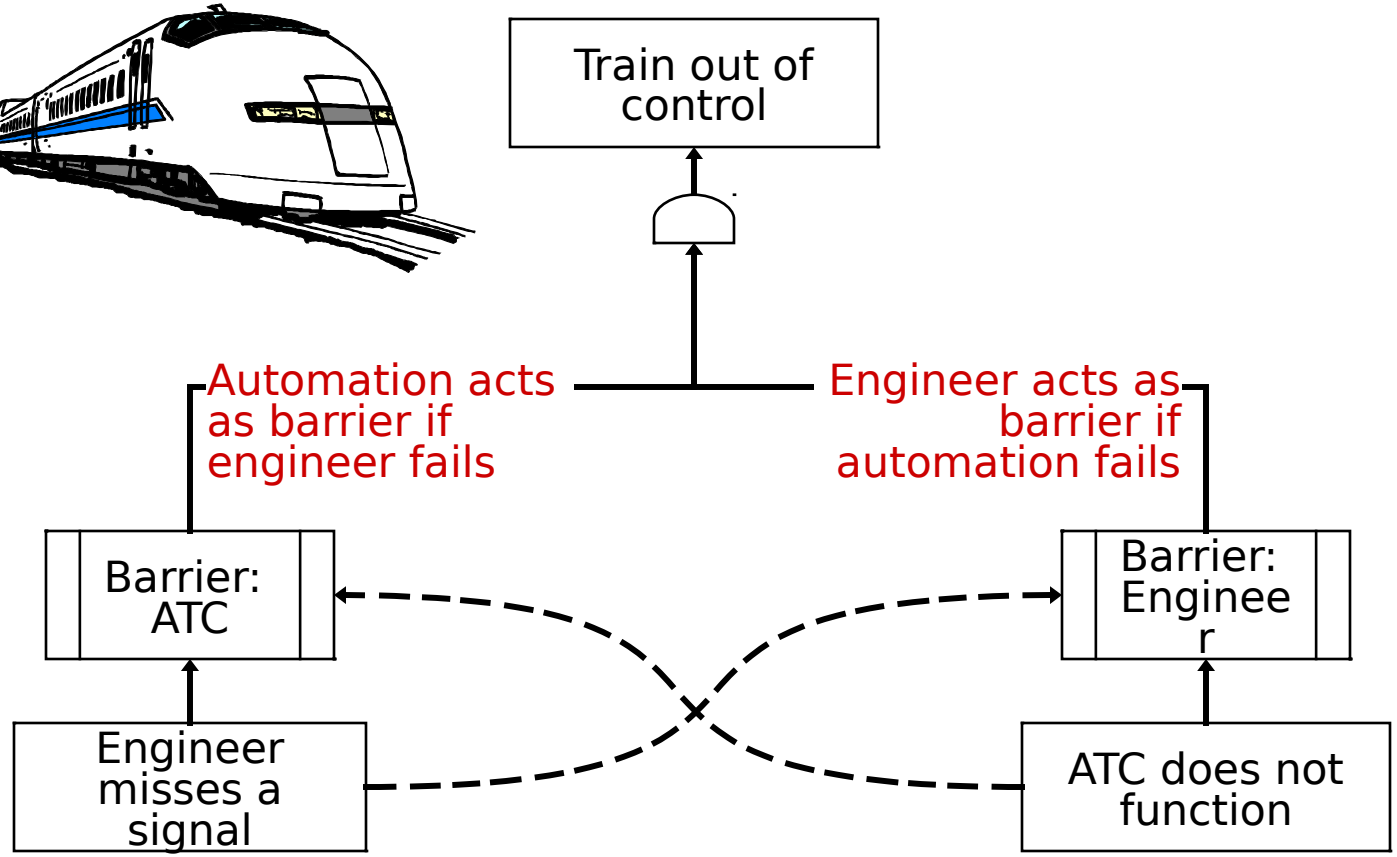
Train accident



Erik Hollnagel, 2003

Double role of barriers

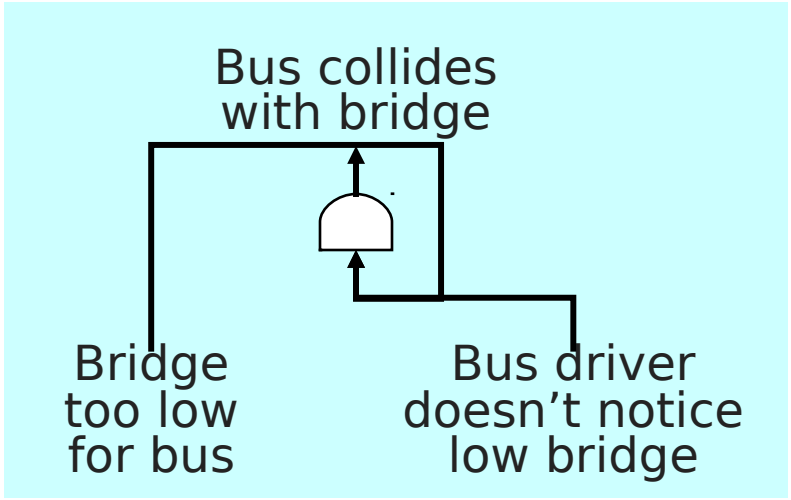


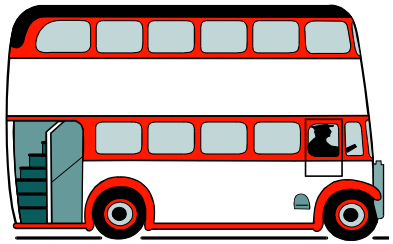

Train out of control
Automation acts as barrier if engineer fails
Engineer acts as barrier if automation fails
Barrier: ATC
Barrier: Enginee r
Engineer misses a signal
ATC does not function

Erik Hollnagel, 2002

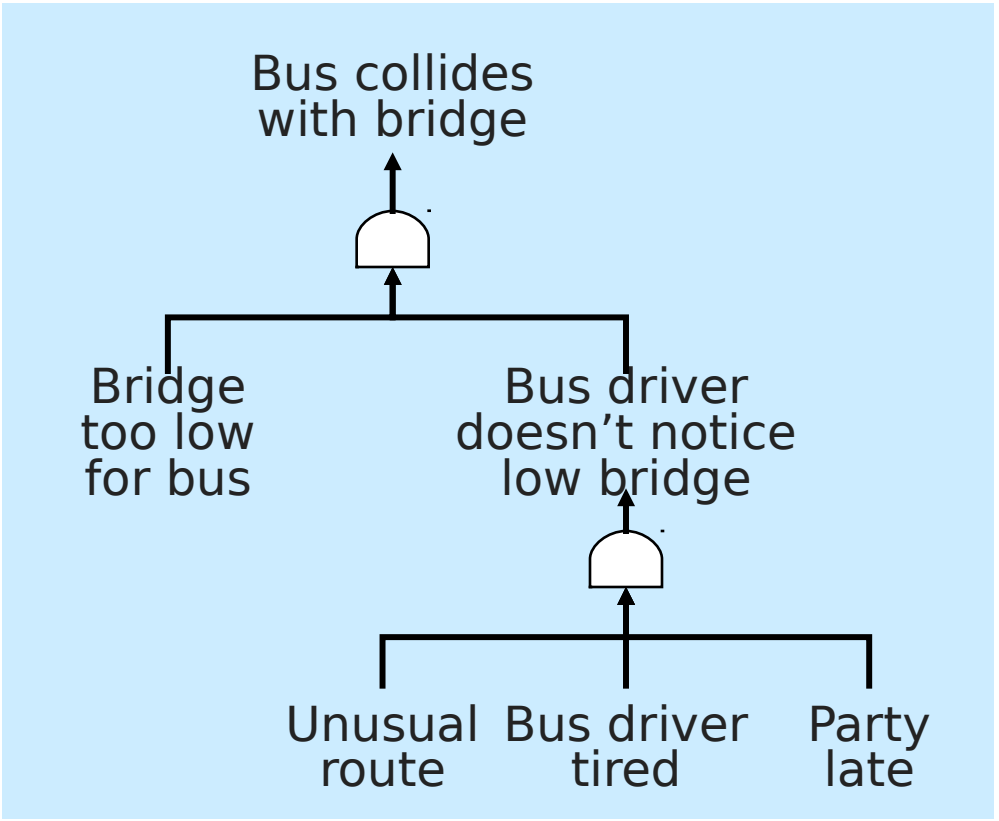
LINKÖPINGS UNIVERSITET

Glasgow bus accident



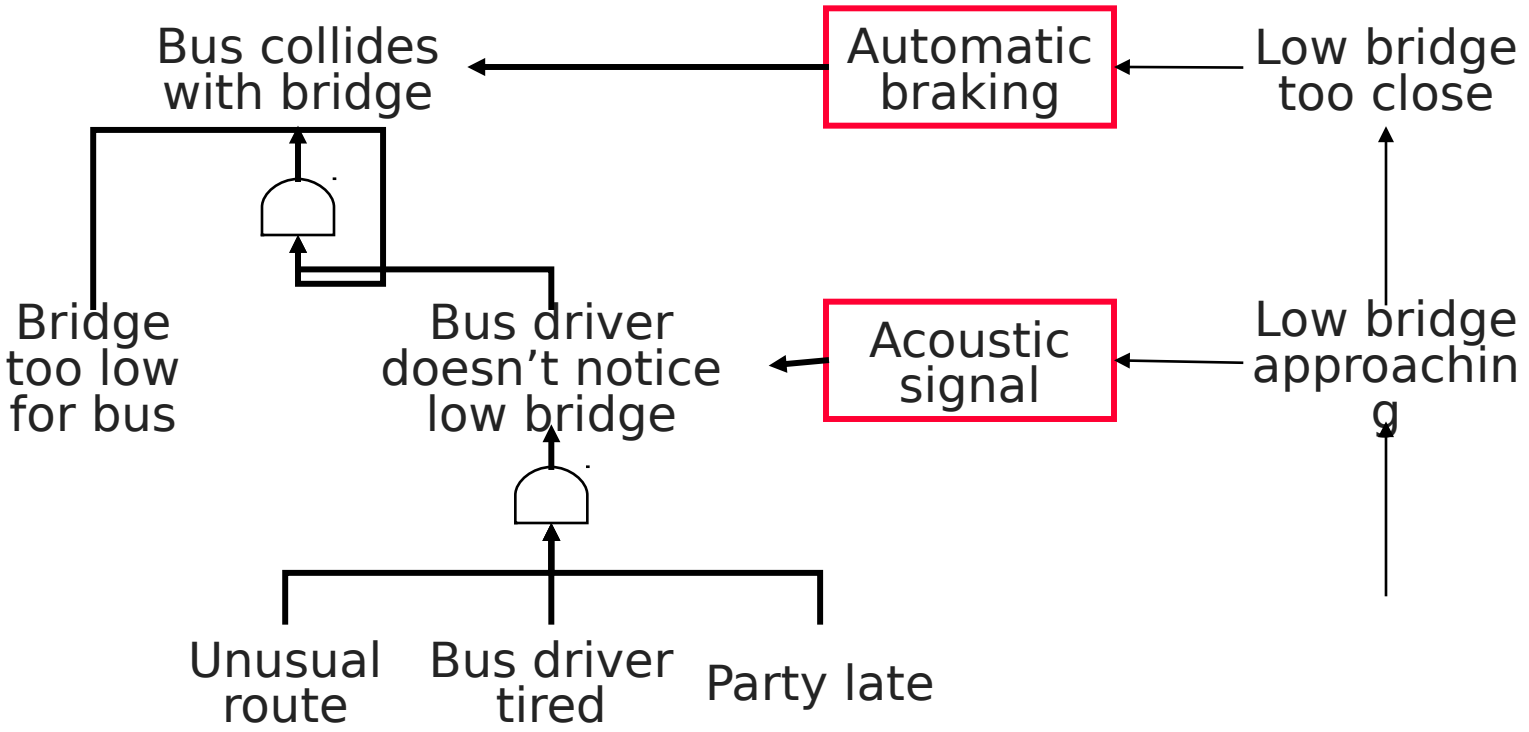


September 18, 1994



Erik Hollnagel, 2002

Glasgow bus accident



Erik Hollnagel, 2002

Barrier evaluation criteria

- Efficiency: how efficient the barrier is expected to be in achieving its purpose.
- Robustness: how resistant the barrier is w.r.t. variability of the environment (working practices, degraded information, unexpected events, etc.).
- Delay: Time from conception to implementation.
- Resources required. Costs in building and maintaining the barrier.
- Safety relevance: Applicability to safety critical tasks.
- Evaluation: How easy it is to verify that the barrier works.
- Other: Maintenance needs; complexity; reusability; ...

Erik Hollnagel, 2002

LINKÖPINGS UNIVERSITET

Evaluation of barrier quality

	Material barriers	Functional barriers	Symbolic barriers	Immaterial barriers
Efficiency	High	High	Medium	Low
Robustness (reliability)	Medium-High	Medium-High	Low-medium	Low
Delay	Long	Long	Medium	Short
Resource needs	Medium-High	Medium-High	Medium	Low
Safety relevance	Low	Medium	Low (uncertain interpretation)	Low
Evaluation	Easy	Medium	Easy	Difficult

Erik Hollnagel, 2002

LINKÖPINGS UNIVERSITET

Requirements for effective barrier functions

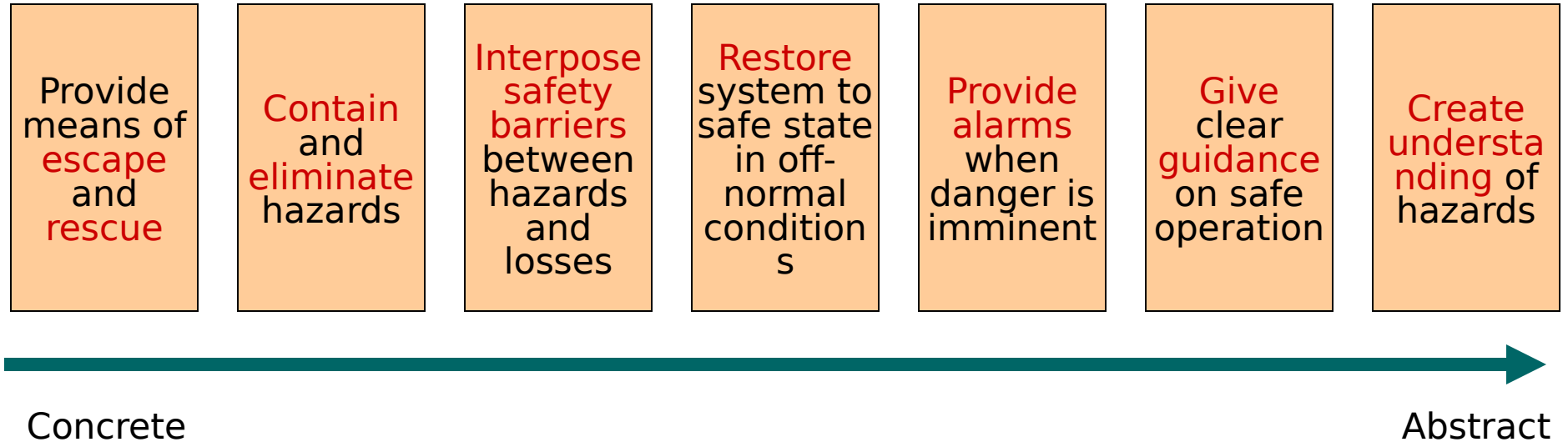
Barrier system	Barrier function relies on	Pre/condition for proper functioning	Reliance on humans
Material	Physical properties	Reliable construction, possibly regular maintenance	Low (maintenance)
Functional	Mechanical	Reliable construction, regular maintenance	Low
	Logical	Verified implementation, adequate security	Low
	Spatio-temporal	Reliable construction, regular maintenance	Low
	Monitoring	Reliable performance of monitor	Medium
Symbolic	Interface design	Valid design specification, verified implementation, systematic updating	Medium
	Information	High-quality interface design, reliable functioning.	High
	Signs, signals and symbols	Regular maintenance, systematic modification,	High
	Permission or authorisation	High compliance by users.	High
Immaterial	Communicative, interpersonal	Nominal working conditions (no stress, noise, distraction, etc.	High
	Rules, cautions, prohibitions	High compliance by users.	High

Erik Hollnagel, 2002

LINKÖPINGS UNIVERSITET

Redundancy in accident prevention

(Reason, 1997)


Provide means of escape and rescue
Contain and eliminate hazards
Interpose safety barriers between hazards and losses
Restore system to safe state in off-normal conditions
Provide alarms when danger is imminent
Give clear guidance on safe operation
Create understanding of hazards
Concrete
Abstract

Erik Hollnagel, 2002

LINKÖPINGS UNIVERSITET

Diversity in accident prevention

Immaterial barrier system

Laws, rules, principles, …

Symbolic barrier system

Signs, signals, procedures, …

Guide humans on safe performance → Need to be interpreted

Functional barrier system

Interlocks, passwords, …

Material barrier system

Walls, guardrails, …

Prevent unsafe acts and their consequences → Do not need to be interpreted

Erik Hollnagel, 2002

LINKÖPINGS UNIVERSITET

Structure of Defences-in-Depth

(Itoh, 2001)

	Help escaping	Contain hazards	Interpose barriers	Restore system	Provide alarms	Give guidance	Create understan-ding
Immaterial							Prescribing
Symbolic					Indicating	Countering, regulating	Permission, communi-cation
Functional			Preventing	Preventing, hindering	Monitoring		
Material	Dissipating	Restoring, Keeping together	Containing, protecting				

Erik Hollnagel. 2002

LINKÖPINGS UNIVERSITET

Conclusions

- Accident model determines analysis and responses
  - “Causes” reflect the assumptions of the underlying models
  - Performance variability management rather than accident / “error” prevention
- The misleading simplicity of “human error”
  - Human performance is inherently variable - but not unreliable
  - Variability reflects work conditions
  - Performance deviations have positive and negative consequences: “errors” as an opportunity for learning.
- Barriers are effective even if causes are unknown or uncertain
  - Distinction between barrier systems and barrier functions
  - Requirements for effective barrier functions.
  - Accident prevention: redundancy and diversity

LINKÖPINGS UNIVERSITET